Citrix® EdgeSight™-Administratordokumentation

Citrix® EdgeSight™ für Endpunkte 5.2
Citrix® EdgeSight™ für XenApp 5.2

Dokumentcode: 9. October 2009 (KM)

Inhalt

Kapitel 3 Verwalten von Servereinstellungen

Kapitel 4 Verwenden von EdgeSight in gemischten Umgebungen

Übersicht

Citrix® EdgeSight™ ist eine Leistungs- und Verfügbarkeitsverwaltungslösung für Endpunkt-, XenDesktop- und XenApp-Systeme. EdgeSight überwacht Anwendungen, Geräte, Sitzungen und das Netzwerk in Echtzeit, sodass Benutzer Probleme schnell analysieren, lösen und proaktiv verhindern können. In diesem Dokument werden die Konfigurations- und Verwaltungsaufgaben beschrieben, die über die Citrix EdgeSight Server Console ausgeführt werden können. Dieses Kapitel enthält eine Beschreibung der primären EdgeSight-Komponenten und der Software-Architektur sowie einen Überblick über die Verwaltungsaufgaben.

Citrix XenApp ist der neue Name von Citrix Presentation Server. In diesem Dokument wird XenApp als der Produktname verwendet und bezieht sich auf XenApp und Presentation Server, wenn nicht anders angegeben.

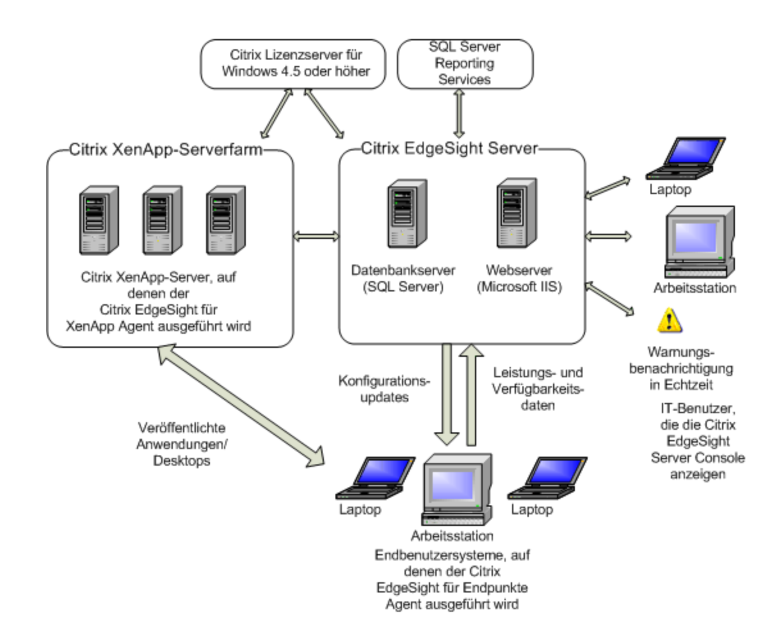
Citrix EdgeSight-Komponenten

Citrix EdgeSight besteht aus den folgenden Komponenten:

- EdgeSight-Agents
- EdgeSight Server
- EdgeSight Server Console
- Citrix Lizenzserver

Für die Überwachung virtueller Desktops sind zusätzliche Komponenten erforderlich, wie unter "EdgeSight-Komponenten für die Überwachung virtueller Desktops" auf Seite 11 beschrieben. Beachten Sie, dass EdgeSight zum Generieren von Verlaufsberichten SQL Server Reporting Services benötigt. Die Systemanforderungen für Agents und Server werden in der *Citrix EdgeSight-Installationsanleitung* beschrieben.

Die folgende Abbildung zeigt die Beziehungen zwischen diesen Komponenten und den zu überwachenden Systemen:



EdgeSight-Agents

EdgeSight-Agents sind Dienste, die auf einem Endbenutzergerät, virtuellen Desktops oder XenApp-Servern ausgeführt werden und Daten erfassen, die sie in eine Datenbank auf dem Client schreiben. Ein Agent sammelt Daten, fasst diese zu Nutzdaten zusammen und sendet die Nutzdaten an EdgeSight Server. Folgende Arten von Agents sind verfügbar:

- EdgeSight für Endpunkte-Agent: Die Endpunktagent-Software ist für Benutzer-Desktop- oder -Laptopumgebungen gedacht. Die Agents arbeiten fortlaufend und diskret auf den Benutzersystemen und erfassen dabei Leistungs-, Ressourcen-, Anwendungs- und Netzwerkdaten. Die erfassten Daten werden in einer lokalen Datenbank gespeichert und in vordefinierten Abständen auf einen EdgeSight-Server hochgeladen. Zur Vereinfachung der Problemlösung können die Daten aber auch direkt von einer Agentdatenbank aus angezeigt werden.#
  #
  Mit Endpunktagentsoftware können auch virtuelle Desktops, die auf XenDesktop 3.0 basieren, überwacht werden, bei denen Daten zwischen Neustarts nicht gespeichert werden. In diesem Fall speichern Agents Daten in einer Remotedatenbank und der EdgeSight-Server fungiert als Datenbankbroker. Weitere Informationen dazu finden Sie unter "EdgeSight-Komponenten für die Überwachung virtueller Desktops" auf Seite 11.

- EdgeSight für virtuelle Desktops Agent: Die Agentsoftware für virtuelle Desktops ist für die Überwachung von auf XenDesktop 4.0 basierenden virtuellen Desktops gedacht. Zusätzlich zur Überwachung von System-, Anwendungs- und Netzwerkleistung sammelt sie ICA-Kanal-Daten einschließlich von XenDesktop-Multimedialeistungsindikatoren, Endbenutzererlebnisdaten und sendet Warnungen über die XenDesktop-Sitzungsleistung. Beachten Sie, dieser Agent nicht den Desktop Delivery Controller (DDC) überwacht.#
  #
  Agents speichern Daten in einer Remotedatenbank und der EdgeSight-Server fungiert als Datenbankbroker. Weitere Informationen dazu finden Sie unter "EdgeSight-Komponenten für die Überwachung virtueller Desktops" auf Seite 11.

- EdgeSight für XenApp Agent: Die XenApp-Agent-Software ist für die Verwendung auf XenApp-Servern gedacht. Die erfassten Daten werden in einer lokalen Datenbank gespeichert und zweimal am Tag auf einen EdgeSight-Server hochgeladen. Zur Vereinfachung der Problemlösung können die Daten aber auch direkt von einer Agentdatenbank aus angezeigt werden. Es gibt zwei Typen von EdgeSight für XenApp Agent:

  - *Standard*-Agents bieten die Ressourcenverwaltungsfunktionen, die Teil von XenApp Enterprise Edition sind. Hierfür ist nur erforderlich, dass Sie eine XenApp Enterprise-Lizenz auf Ihrem Citrix Lizenzserver haben. Der Agent zeichnet Informationen zur Client- und Serverleistung und zur Anwendungsnutzung auf.

  - *Erweiterte* Agents bieten den vollen Funktionsumfang von EdgeSight für XenApp. Hierfür benötigen Sie entweder eine XenApp Platinum Edition-Lizenz oder eine EdgeSight für XenApp-Lizenz auf Ihrem Citrix Lizenzserver. Der Agent zeichnet Informationen zu Benutzersitzungen, zur Client- und Serverleistung, zur Anwendungsverwendung und zu den Netzwerkverbindungen auf.

Hinweis: Resource Manager ist eine Version mit eingeschränkter Funktionalität von EdgeSight für XenApp, deren Funktionsumfang der XenApp-Komponente Resource Manager entspricht. Resource Manager verwendet die Standardversion des EdgeSight für XenApp Agents.

EdgeSight Server

EdgeSight Server erfasst Daten von den verteilten Agents und ermöglicht es Administratoren, die Daten zum Identifizieren möglicher Probleme im Unternehmen und zum Zweck der Problemlösung anzuzeigen. EdgeSight Server besteht aus den folgenden Komponenten:

- Webserver: Die Webserverkomponente empfängt die Datenuploads von den Agents und zeigt in der EdgeSight Server Console in einer Vielzahl von Standardberichten die entsprechenden Leistungs- und Verfügbarkeitsinformationen an.
- Datenbankserver: Die Datenbankserverkomponente speichert die hochgeladenen Daten von den Agents und dient als Datenquelle für SQL Server Reporting Services.
- Berichtserver: Die Berichtserverkomponente generiert Leistungs- und Verfügbarkeitsinformationen in Form von Berichten. Der Berichtserver verwendet Microsoft SQL Server Reporting Services.

In Umgebungen, in denen EdgeSight für Endpunkte Agents virtuelle Desktops in einem Pool überwachen, sind zusätzliche Komponenten erforderlich:

- EdgeSight-Agentdatenbankserver: Speichert Daten von Agents, die auf virtuellen Desktops in Pools ausgeführt werden. Der EdgeSight-Webserver enthält Datenbankbrokerkomponenten, über die Agents eine Verbindung zu einem Agentdatenbankserver herstellen. Die Datenbankbrokerkomponenten werden standardmäßig installiert. Weitere Informationen dazu finden Sie unter "EdgeSight-Komponenten für die Überwachung virtueller Desktops" auf Seite 11.
- Dateifreigabe für Agentdaten: Die Dateifreigabe für Agentdaten bietet Speicherplatz für Dateien wie Protokolldateien und INI-Dateien, die nicht auf dem EdgeSight-Agentdatenbankserver gespeichert werden.

EdgeSight Server Console

Für die Interaktion zwischen Administrator und EdgeSight Server steht die EdgeSight Server Console zur Verfügung. Die Konsole ist ein leistungsfähiges und flexibles Tool zum Anzeigen von Leistungs- und Verfügbarkeitsinformationen auf der Basis der von den verteilten Agents erfassten Daten. Sie können die Konsole öffnen, indem Sie in einem Webbrowser die URL für den EdgeSight-Server und auf der Anmeldeseite die erforderlichen Anmeldeinformationen eingeben. Administratoren können die Konsole über die folgende URL öffnen:

`http://`*`Servername`*`/edgesight/app/default.aspx`

Die EdgeSight Server Console besteht aus den folgenden Komponenten:

- Registerkarten: Über die Registerkarten im oberen Teil des Inhaltsbereichs können Sie auswählen, welche Daten angezeigt werden sollen und welche Operation Sie durchführen möchten. Die meisten Informationen in dieser Dokumentation beziehen sich auf die Registerkarte "Konfiguration". Es gibt folgende Registerkarten:
    - Einführung: Diese Registerkarte enthält Übersichtsinformationen für alle Registerkarten. Klicken Sie auf die Namen der Registerkarten, um Beschreibungen ihrer Funktionen anzuzeigen. Mit einem Kontrollkästchen können Sie festlegen, ob diese Registerkarte bei zukünftigen Anmeldungen noch angezeigt werden soll.
    - Überwachen: Auf dieser Registerkarte können Sie in Echtzeit die Leistungsindikatoren auf bestimmten Geräten überwachen und Informationen zu Warnungsbedingungen anzeigen.
    - Fehlerbehebung: Auf dieser Registerkarte können Sie mit den Tools zur Fehlerbehebung und den Echtzeitberichten Fehler in Echtzeit beheben. In Echtzeitberichten werden Daten verwendet, die direkt aus Agentdatenbanken stammen.
    - Planen und Verwalten: Auf dieser Registerkarte finden Sie zusammenfassende Berichte, die Ihnen einen Überblick über Ihre Umgebung geben. Zusammenfassende Informationen können zu Geräten, XenApp Server-Computern, Benutzern, Prozessen, Websites und Transaktionen angezeigt werden.
    - Durchsuchen: Auf dieser Registerkarte können Sie Listen von Berichten durchsuchen und Berichte anzeigen. Außerdem können Sie Berichtseigenschaften und Abonnements anzeigen.
    - Konfigurieren: Mit den Optionen auf dieser Registerkarte können Sie Ihr Benutzerprofil bearbeiten, Unternehmen konfigurieren (Agentoptionen, Warnungen, Geräte und Sicherheitseinstellungen), Server konfigurieren (Lizenzierung, Authentifizierung, Datenbankoptimierung und Unternehmenserstellung) und den Serverstatus überwachen (Nachrichten, Aufträge, Dienste und Agentdatenbankbroker).
- Menüleiste: Über die Menüleiste oberhalb des Inhaltsbereichs können Sie häufige Operationen auf der aktuellen Seite ausführen. So können Sie z. B. Ihrer Liste der bevorzugten Berichte eine Seite hinzufügen, die Anzeige einer Seite aktualisieren oder eine Seite drucken. Wenn ein Bericht angezeigt wird, können Sie den Bericht der Liste der bevorzugten Berichte hinzufügen oder diesen Bericht abonnieren.

- Filterleiste: Über die Filterleiste können Sie die Berichtsdaten im jeweils ausgewählten Bericht filtern. Je nach ausgewähltem Bericht stehen u. a. folgende Filterkriterien zur Wahl: Abteilung, Gruppe, Zeitraum, Prozess, Gerät, Benutzer und Site. Durch das Filtern von Daten können Sie Informationen nach konkreten Klassen von Prozessen, Geräten oder Benutzern isolieren und so Probleme und Trends schnell identifizieren. Sie können auch Daten auf Seiten filtern, die keine Berichte sind. Auf diese Weise ist es z. B. möglich, die Daten in der aktuellen Warnungsliste oder die Daten auf den Verwaltungs- und Konfigurationsseiten zu filtern. Klicken Sie zum Anwenden der Filterparameter auf **OK**.
- Link "Hilfe": Durch Klicken auf den Link "Hilfe" in der Konsole oben rechts können Sie die kontextabhängige Onlinehilfe aufrufen. Neben diesen kontextabhängigen Hilfeinformationen enthält das Hilfesystem auch Referenzmaterial, wie z. B. ein Glossar zu den Berichtsparametern und eine Definition der SQL-Ansichten.

Lizenzserver

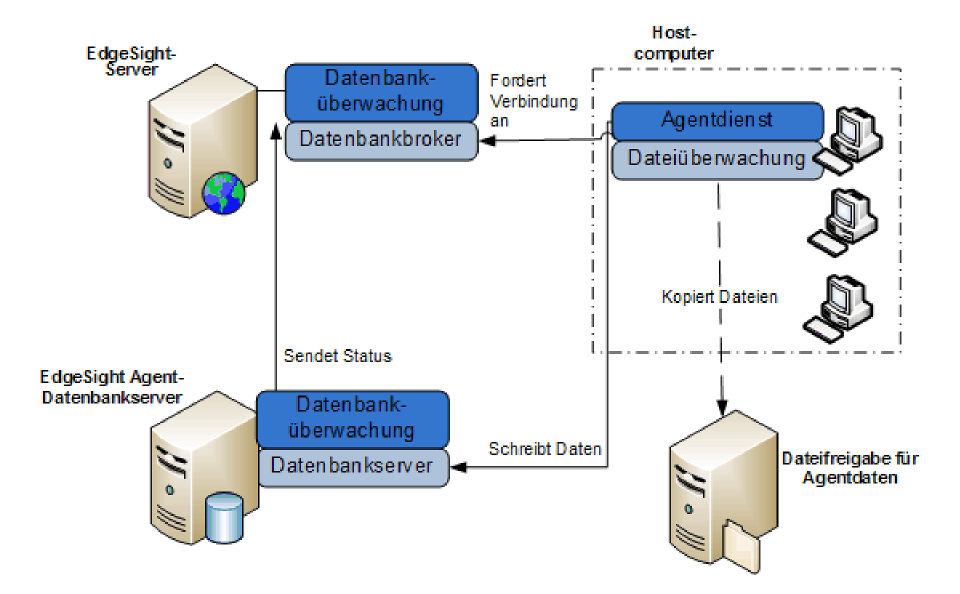
Über Citrix Lizenzserver für Windows 11.6 oder höher werden EdgeSight-Agents Lizenzen bereitgestellt, mit denen diese Daten auf einen EdgeSight-Server hochladen können. Der Lizenzserver kann sich überall im Netzwerk befinden, solange er von der Webserverkomponente des EdgeSight-Servers aus und durch die XenApp Server-Agents erreichbar ist. Ein einzelner Lizenzserver kann von mehreren Citrix Produkten, auch mehreren EdgeSight-Servern, gemeinsam genutzt werden.

Hinweis: Der Lizenzserver und die EdgeSight-Lizenzdateien sollten bereits vorhanden sein, bevor Sie EdgeSight bereitstellen, um so Verzögerungen beim Upload von Daten zu vermeiden.

Für XenApp Server-Agents und Endpunktagents müssen separate Lizenzen erworben werden. Dies gilt auch dann, wenn beide Agentarten mit demselben Server verknüpft sind. Alle Agent-Lizenzdateien (z. B. `CESEP_*.lic`) müssen sich im Ordner "MyFiles" des Lizenzserververzeichnisses auf dem EdgeSight-Server befinden. Weitere Informationen zum Verwalten von Lizenzen finden Sie unter "Verwalten von Lizenzen" auf Seite 65.

EdgeSight-Komponenten für die Überwachung virtueller Desktops

Wenn Sie mit EdgeSight virtuelle Desktops überwachen, bei denen Daten während Neustarts nicht gespeichert werden, sind zusätzliche Komponenten für das Speichern von Agentdaten erforderlich. Die folgende Abbildung zeigt die Beziehungen zwischen diesen Komponenten und den zu überwachenden Systemen:



Folgende Komponenten sind für die Überwachung virtueller Desktops erforderlich:

- EdgeSight Server: Jede EdgeSight Server-Installation umfasst Datenbankbroker- und Datenbankmonitorkomponenten, die Datenbankverbindungsinformationen an EdgeSight-Agents, die auf virtuellen Desktops in einem Pool ausgeführt werden, weitergeben und den EdgeSight-Agentdatenbankserver nach Registrierungs- und Statusinformationen abhören.
- EdgeSight-Agentdatenbankserver: Auf den Datenbankservern werden die Daten gespeichert, die EdgeSight-Agents auf virtuellen Desktops sammeln. Der Datenbankmonitor auf jedem Server kommuniziert mit dem EdgeSight-Server, um regelmäßig Verfügbarkeits- und Statusinformationen zu senden.
- Dateifreigabe für Agentdaten: Die Dateifreigabe speichert Agentdateien wie Protokolldateien und INI-Dateien, die nicht auf dem EdgeSight-Agentdatenbankserver gespeichert werden.

- EdgeSight-Agents: Die EdgeSight-Agents sammeln Leistungsdaten auf den virtuellen Desktops, auf denen sie installiert sind. Während der Installation geben Sie den Pfad zur Dateifreigabe für Agentdaten an sowie welcher EdgeSight-Server Datenbankverbindungsinformationen zur Verfügung stellt. Welcher Agent installiert wird, hängt von der Version der virtuellen Desktops in Ihrer Umgebung ab. Der EdgeSight für Endpunkte Agent ist für die Überwachung von System-, Anwendungs- und Netzwerkleistung auf virtuellen Desktops, die auf XenDesktop 3.0 basieren, gedacht. Der EdgeSight für virtuelle Desktops Agent ist für die Überwachung von Sitzungs-, System-, Anwendungs- und Netzwerkleistung auf virtuellen Desktops, die auf XenDesktop 4.0 basieren, gedacht.

Die EdgeSight-Komponenten funktionieren in größeren Umgebungen, die Citrix Provisioning Server und eventuell XenServer enthalten. In der *Citrix EdgeSight-Installationsdokumentation* finden Sie Informationen zu den Systemanforderungen.

Weitere Informationen über die Verwendung der EdgeSight Server Console zur Überwachung des Status von Pools, Agentdatenbankservern und Datenbankbrokermeldungen finden Sie unter "Anzeigen des Status des Agentdatenbankbrokers" auf Seite 79.

Begriffserläuterungen

Ein *Unternehmen* ist die primäre Organisationseinheit auf einem EdgeSight-Server. Ein einzelner Server kann mehrere Unternehmen unterstützen. Unternehmen sind in *Abteilungen* unterteilt. Abteilungen sind in einer hierarchischen Struktur organisiert mit einer Standardstammabteilung (Alle) und gerätspezifischen Unterabteilungen (XenApp-Farmen, XenDesktop-Farmen und Endpunkte), die bei der Installation erstellt werden. Die Struktur der Unterabteilungen von XenApp-Farmen und Desktopfarmen wird von den Farmen bestimmt und kann nicht mit der EdgeSight Server Console geändert werden. Zusätzliche Endpunktunterabteilungen können automatisch erstellt werden, wenn Agenten beim Server registriert werden, oder sie können manuell erstellt werden. Die Konfigurationsinformationen werden abteilungsweise mit den Agents verknüpft. Jede Abteilung entspricht einem Satz von Systemen, auf denen EdgeSight-Agents ausgeführt werden. Diese Systeme werden als *Geräte* bezeichnet.

Zusätzlich zur Strukturierung nach Abteilung können Sie Geräte auch nach benutzerdefinierten *Gruppen* organisieren. Eine benutzerdefinierte Gruppe ist eine vom Benutzer definierte Zusammenstellung von Geräten. Die Mitgliedschaft in einer Gruppe kann sich nach den verknüpften Abteilungen, den Gerätemerkmalen oder Abfragen richten.

Sie können nicht nur Gerätegruppen, sondern auch *Benutzergruppen* erstellen, die Sammlungen von XenApp-, XenDesktop- oder Endpunktbenutzern sind. Viele Berichte mit Daten zum Benutzererlebnis können nach Benutzergruppen gefiltert werden, sodass Sie die Systemleistung für eine Gruppe von Benutzern mit spezifischen Eigenschaften überwachen können.

EdgeSight Console-*Benutzer* melden sich bei der Konsole an, um Berichte anzuzeigen oder Verwaltungsaufgaben auszuführen. (Beachten Sie, dass sich in Berichten der Begriff "Benutzer" auf XenApp- oder XenDesktop-Benutzer bezieht, die mit einer Sitzung verknüpft sind.) Jedem Konsolenbenutzer wird eine *Rolle* (z. B. die Standardrolle "Administrator" oder "Berichts-Viewer") zugewiesen, zu der jeweils ein Satz *Berechtigungen* gehört. Diese Berechtigungen bestimmen, welche Aktionen ein Benutzer ausführen kann und welche Seiten in der Konsole angezeigt werden. So ist ein Benutzer mit der Rolle "Berichts-Viewer" zwar berechtigt, Berichte einzusehen, er kann aber keine Seiten im Ordner "Unternehmenseinstellungen" oder "Servereinstellungen" anzeigen und auch keine Verwaltungsaufgaben auf dem Server ausführen.

Benutzer können von der Konsole aus auf Berichte zugreifen oder Berichte auf der Basis eines *Abonnements* erhalten. Innerhalb eines Abonnements können die Berichte entweder per E-Mail gesendet oder auf eine Dateifreigabe geladen werden. (Auf diese Weise lassen sich effektiv und gezielt Informationen an Personen in der Organisation verteilen, ohne dass diese sich bei der Konsole anmelden müssen.) Die Verteilung der abonnierten Berichte erfolgt nach einem festgelegten Zeitplan.

EdgeSight-Architektur

In diesem Abschnitt werden die folgenden grundlegenden Aspekte der EdgeSight-Architektur vorgestellt:

- Agenttypen
- Agentprozesse
- Art der erfassten Agentdaten
- Art und Weise, wie die Agentdaten gespeichert, zusammengestellt und auf den EdgeSight-Server hochgeladen werden

Agenttypen

EdgeSight bietet folgende Agenttypen:

- EdgeSight für Endpunkte: Endpunkt-Agents bieten Überwachungs- und Datensammlungsfunktionen für Endpunktgeräte und virtuelle Desktops, die auf XenDesktop 3.0 basieren.
- EdgeSight für virtuelle Desktops: Agents für virtuelle Desktops bieten Überwachungs- und Datensammlungsfunktionen für Endpunktgeräte und virtuelle Desktops, die auf XenDesktop 3.0 basieren.
- EdgeSight für XenApp, Standard: Standard-Agents bieten die Ressourcenverwaltungsfunktionen, die Teil von XenApp Enterprise Edition sind. Hierfür ist nur erforderlich, dass Sie eine XenApp Enterprise-Lizenz auf Ihrem Citrix Lizenzserver haben.
- EdgeSight für XenApp, Erweitert: Erweiterte Agents bieten den vollen Funktionsumfang von EdgeSight für XenApp. Hierfür benötigen Sie entweder eine XenApp Platinum Edition-Lizenz oder eine EdgeSight für XenApp-Lizenz auf Ihrem Citrix Lizenzserver.

Agentprozesse

Der EdgeSight-Agent beinhaltet die folgenden Schlüsselprozesse:

Citrix System Monitoring Agent-Dienst

- Dieser Prozess erfasst Daten (Ressourcennutzung, Ereignisse und Hardwareänderungen) von einem Endbenutzergerät, einer XenDesktop-Instanz oder einem XenApp-Server.
- Er kommuniziert bei Konfigurationsdownloads und Nutzdatenuploads über Port 9035 mit dem EdgeSight-Server.
- Außerdem fordert er für Agents in Desktoppoolumgebungen eine Verbindung zu einer Remotedatenbank an.

Der Firebird-Dienst-Prozess speichert die Daten, die auf dem Benutzergerät oder dem XenApp-Server erfasst wurden, in der lokalen Agentdatenbank.

Wenn ein Agent auf virtuellen Desktops in einer gepoolten Umgebung installiert wird, kopiert der Dateimonitor-Prozess Dateien auf eine Dateifreigabe für Agentdaten bzw. ruft sie von dort ab.

Für den System-Overhead für die Agentprozesse gelten die im Folgenden genannten Werte. Es handelt sich hierbei um Durchschnittswerte, die je nach Computer und Umgebung abweichen können. (Beachten Sie, dass Agents, die auf virtuellen Desktops installiert sind, weniger Speicherplatz beanspruchen, weil Sie eine Remotedatenbank verwenden.)

- CPU-Overhead: 1 % bis 2 %
- Beanspruchter Arbeitsspeicher: 30 MB bis 35 MB
- Netzwerknutzung pro Tag: 200 KB
- 40 bis 250 MB Festplattenspeicher

Erfassung von Agentdaten

Die Datenerfassung erfolgt typischerweise während der normalen Systemnutzung, um so sicherzustellen, dass die erfassten Daten die Systemverfügbarkeit und -leistung korrekt darstellen und nicht durch lange Inaktivitätszeiten verfälscht werden. Einige Parameter, wie z. B. die Statistik zu kritischen Anwendungs- und Dienstressourcen, werden nur erfasst, wenn der Benutzer das System aktiv nutzt. In der Agentdatenbank werden die folgenden Datenarten erfasst und gespeichert:

- Leistungsdaten
- Ereignisgesteuerte Daten
- XenApp- und Xen Desktop-Daten

Leistungsdaten

Leistungsdaten beinhalten Daten für Systemmessobjekte, wie die CPU- oder Arbeitsspeichernutzung, die im normalen Systembetrieb auftreten. EdgeSight sammelt u. a. folgende Daten:

- CPU-Auslastung
    - CPU-Nutzung in einem bestimmten Zeitraum
    - Vergleich der CPU-Nutzung zwischen mehreren Geräten
    - Verfolgung der CPU-Auslastung
    - Welche Prozesse verbrauchen die meiste CPU?

- Speicherauslastung
  - Wie viel RAM wird beansprucht?
  - Welche Anwendungen verbrauchen den meisten Speicher?
  - Welche Computer haben am wenigsten freien Arbeitsspeicher?
- Festplattenauslastung
  - Wie viel Festplattenspeicherplatz ist verfügbar?
  - Bei welchen Systemen gibt es potenziell Festplattenprobleme?
  - Welche Computer haben am wenigsten freien Festplattenspeicher?

Ereignisgesteuerte Daten

Zu den ereignisgesteuerten Daten gehören Parameter, die von einem auf dem Benutzersystem stattfindenden Ereignis generiert werden. Dies ist z. B. der Fall, wenn ein Benutzer eine Anwendung startet und sie zu nutzen beginnt oder wenn eine Socket-Verbindung hergestellt wird. EdgeSight sammelt u. a. folgende Daten:

- Anwendungsprobleme (Fehler, Abstürze und nicht mehr reagierende Anwendungen)
  - Welche Fehlermeldung wurde angezeigt?
  - Wann ist der Fehler aufgetreten?
  - Wie oft ist der Fehler aufgetreten?
  - Welches System hat den Fehler ausgegeben?
  - Was wurde noch auf dem System ausgeführt, als der Fehler auftrat?
- Anwendungsnutzung (besonders hilfreich bei der Überwachung der Lizenzeinhaltung)
  - Wie lange wurde die Anwendung im Speicher ausgeführt?
  - Wie lange war die Aktivitäts- und die Inaktivitätszeit?
  - Welche Anwendungen werden von welchen Benutzern verwendet?

- Netzwerkverbindung
  - Reaktionszeit für die Netzwerkkommunikation
  - Durchschnittliche Geschwindigkeit des Netzwerks
  - Menge des beanspruchten Netzwerkvolumens
  - Roundtrip-Zeit für bestimmte Verbindungen
  - Systeme mit der größten Verzögerung
  - Anwendungen, die das größte Volumen generieren
  - Server mit der langsamsten Reaktionszeit
  - Im Netzwerk verwendete Protokolle
  - Besuchte Sites und neue Sites

XenApp- und Xen Desktop-Daten

XenApp-Daten beinhalten u. a. Angaben zu folgenden Parametern:

- EUEM-Daten (End User Experience Monitoring = Überwachung des Endbenutzererlebnisses) einschließlich von Sitzungsleistung, ICA-Roundtrip und Client- und Serverstartzeiten. Diese ICA-Roundtrip-Daten ersetzen die Sitzungslatenzdaten, die von älteren Versionen der Agents gesammelt wurden.
- Sitzungsaktivität, z. B. aktive, inaktive und Gesamtanzahl der Sitzungen
- Automatische Wiederverbindungen von Sitzungen
- Bandbreite für ICA-Sitzungseingabe und -ausgabe für Audio, Video, Drucker und Dateioperationen
- Zustand und Verfügbarkeit des IMA-Dienstes
- Ressourcennutzung, z. B. Arbeitsspeicher und CPU, für Gruppen und Benutzer
- Netzwerkverzögerung bei Sitzungen und Roundtrip-Zeit für Gruppen und Benutzer
- Active Application Monitoring-Daten, z. B. Reaktionszeiten und Fehler bei Anwendungstests.

XenDesktop-Daten beinhalten u. a. Angaben zu folgenden Parametern:

- ICA-Kanal-Daten einschließlich von XenDesktop-Multimedia-Leistungsindikatoren
- Endbenutzererlebnismessobjekten
- XenDesktop-Sitzungsleistung

Zusammenfassung der Agentdaten

Die Agentdaten werden wie folgt zusammengefasst:

- Daten werden alle fünf bis 15 Sekunden erfasst und in der lokalen Agentdatenbank gespeichert. Endpunktdaten werden alle fünf Sekunden und XenApp-Daten werden alle 15 Sekunden gespeichert.
- Alle 20 Minuten werden die erfassten Daten in Fünf-Minuten-Abschnitten zusammengefasst und an einem neuen Ort in der lokalen Agentdatenbank gespeichert.
- Einmal pro Tag werden die Fünf-Minuten-Abschnitte neu zu Ein-Stunden-Abschnitten zusammengestellt und entsprechend dem konfigurierten Upload-Zeitplan auf den EdgeSight Server hochgeladen.
- Die Daten bleiben drei Tage lang in der Agentdatenbank gespeichert, um die Anzeige von Verlaufsdaten zu ermöglichen. Nach Ablauf dieser Zeit werden die Daten aus der Agentdatenbank gelöscht. Die Einstellung, wie lange die Daten aufbewahrt werden, kann aber durch Bearbeiten der Agenteigenschaften geändert werden.

Wenn die Agentsoftware auf einem mobilen Gerät installiert ist oder das Gerät keine Verbindung zum EdgeSight-Server herstellen kann, wird eine Zusammenfassung der Daten fünf Tage für XenApp-Server und 29 Tage für Endpunkte und virtuelle Desktops aufbewahrt oder bis das Gerät wieder zum Server hochladen kann. Die Dauer der Datenaufbewahrung können Sie Ihren Erfordernissen entsprechend konfigurieren. Weitere Informationen dazu finden Sie in der Onlinehilfe im Abschnitt "Assistent für Agenteigenschaften".

Upload von Agentdaten

Bei der Erstinstallation des Agents registriert dieser sich selbst beim Server und ruft Informationen dazu ab, wann die Daten laut Zeitplan auf den Server hochgeladen werden und welche Daten der Server anfordert.

Bei Verwendung der Standardworkerkonfiguration "Leistungsupload" werden die Daten von der Agentdatenbank auf den EdgeSight-Server hochgeladen. Endpunkt-Agents laden standardmäßig einmal am Tag Daten hoch, XenApp-Agents laden Daten zweimal am Tag hoch und Agents für virtuelle Desktops laden Daten alle anderthalb Stunden hoch. Falls erforderlich, können Sie die Agents so konfigurieren, dass der Upload häufiger erfolgt. So könnte z. B. ein Datenupload für die Mittagszeit geplant werden, um so die morgendliche Aktivität auszuwerten. Weitere Informationen zu Workerkonfigurationen finden Sie unter "Konfigurieren, Terminieren und Ausführen von Workern" auf Seite 53.

Ein typischer Datenupload für einen EdgeSight für Endpunkte-Agent ist 80 KB groß. Datenuploads für einen EdgeSight für XenApp Agent sind normalerweise größer, da mehr Daten erfasst werden. Solche Datenuploads können bis zu 300 KB groß sein. Die genaue Größe der Datenuploads hängt von verschiedenen Faktoren ab, u. a. den Agenteigenschaften und dem Nutzungsprofil des Systems, das den Agent hostet.

Der Prozess des Datenuploads lässt sich wie folgt zusammenfassen:

1. Der EdgeSight-Agent kontaktiert den EdgeSight-Server, um anhand des Zeitpunkts des letzten erfolgreichen Uploads herauszufinden, welche Daten angefordert werden.
2. Der Agent fragt die lokale Datenbank ab und stellt die abgefragten Nutzdaten in Ein-Stunden-Abschnitten zusammen.
3. Die Nutzdaten werden komprimiert und über HTTP oder HTTPS an die Webserverkomponenten von EdgeSight Server gesendet. (HTTPS wird verwendet, wenn der Agent so konfiguriert ist, dass die Verbindung durch SSL gesichert wird. SSL-Unterstützung muss auf dem Server aktiviert sein und auf dem Server, auf dem die EdgeSight-Website ausgeführt wird, muss ein gültiges SSL-Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle vorhanden sein.)
4. Die Nutzdaten werden im lokalen Datenordner gespeichert, von wo aus sie vom EdgeSight Script Host (RSSH) abgerufen und verarbeitet werden.

Verwaltungsaufgaben

Verwaltungsaufgaben können Sie nur ausführen, wenn Ihnen die Rolle "Administrator" zugewiesen wurde oder Sie Administratorberechtigungen besitzen. Weitere Informationen zur Rolle "Administrator" und zu Berechtigungen finden Sie in Kapitel 2, "Erstellen von Benutzern und Zuweisen von Rollen" . Die Verwaltungsaufgaben unterteilen sich in unternehmens- und in serverspezifische Aufgaben.

Serverweite Einstellungen werden Benutzern nur dann angezeigt und können auch nur dann von ihnen bearbeitet werden, wenn sie die Berechtigung "Servereinstellungen verwalten" besitzen. Diese Berechtigung wird dem Superuser bei der Installation automatisch eingeräumt. Allen anderen Benutzern muss diese Berechtigung explizit gewährt werden, wobei dies beim Erstellen oder Bearbeiten des Benutzers und nicht durch eine Rollenzuweisung erfolgt.

Unternehmenseinstellungen wirken sich lediglich auf ein einzelnes Unternehmen aus, während Servereinstellungen für alle Unternehmen relevant sind, die auf dem Server residieren. Unternehmenseinstellungen enthalten sowohl Server- als auch Agenteinstellungen.

Verwaltungsaufgaben in Unternehmen

In Unternehmen fallen u. a. folgende Verwaltungsaufgaben an:

- Festlegen, wann und wie Worker auf Geräten ausgeführt werden
- Festlegen, wann und wie Agents Daten erfassen und wie lange die Daten aufbewahrt werden
- Einrichten einer Echtzeitbenachrichtigung zu Warnungsbedingungen durch Erstellen und Implementieren von Regeln und Aktionen für Warnungen
- Organisieren der Geräte nach Abteilung oder benutzerdefinierter Gruppe
- Organisieren der Benutzer in Gruppen zum Zweck der Berichtsfilterung
- Festlegen, welche Daten für ausgewählte Computer im Echtzeit-Dashboard angezeigt werden
- Festlegen, wie Berichte auf der Grundlage von Abonnements automatisch an Benutzer verteilt werden
- Einrichten des Konsolenbenutzerzugriffs und der Berechtigungen
- XenApp-Farm-Authentifizierung
- Festlegen der IP-Bereiche für die Filterung des Netzwerks nach Unternehmenshosts oder Hosts in externen Netzwerken

- Festlegen, wie Anwendungen in Kategorien zu Berichtszwecken gruppiert werden
- Festlegen, wie Anwendungen nach Software-Anbietern zu Berichtszwecken gruppiert werden
- Festlegen von Unternehmenseinstellungen für die Zeitzone und Einstellungen für die Agentregistrierung

Verwaltungsaufgaben auf dem Server

Für Server fallen u. a. folgende Verwaltungsaufgaben an:

- Überwachen des Gesamtserverstatus
- Verwalten der Authentifizierungsprovider
- Erstellen von Unternehmen
- Überwachen von Lizenzinformationen und Aktualisieren von Lizenzservernamen und -ports
- Konfigurieren von Servervorgängen, z. B. Agentunterstützung, Benachrichtigungen, Timeouts, Datenuploads, Verarbeitung von Absturzdateien, SSL-Unterstützung und SNMP-Trap-Ports
- Überwachen des Status von Diensten
- Überwachen und Organisieren nicht verwalteter Geräte (Geräte, auf denen ein Agent installiert ist, der nicht mit einem Unternehmen oder einer Abteilung verknüpft ist)
- Konfigurieren der Serverauthentifizierung bei Reporting Services
- Erstellen und Pflegen von Zeitplänen für das Generieren von Berichten
- Konfigurieren und Überwachen von Parametern für die Datenbankoptimierung
- Konfigurieren und Überwachen von Datenbankwartungsaufgaben
- Anzeigen des Status des Agentdatenbankbrokers
- Anzeigen von Nachrichten zu Serverereignissen und Fehlermeldungen
- Anzeigen von Citrix EdgeSight-Installationspfaden und Softwareversionen

Denken Sie bei der Verwendung dieses Dokuments daran, dass Sie auf jeder EdgeSight Server Console-Seite auf die kontextbezogene Hilfe zugreifen können. Die Hilfethemen enthalten detaillierte Anweisungen zum Ausführen häufiger Aufgaben.

Roadmap für Verwaltungsaufgaben

Bei der Erstkonfiguration von EdgeSight mit dem Assistenten für das Setup nach der Installation legen Sie explizit eine Reihe wichtiger Betriebsparameter für EdgeSight Server fest, darunter ein erstes (übergeordnetes) Unternehmen, ein Superuser-Konto, das auf alle Unternehmen auf einem Server zugreifen und neue Benutzer erstellen kann, E-Mail-Einstellungen zum Senden von Serverbenachrichtigungen und einen Port für die Kommunikation mit dem Lizenzserver. Neben diesen explizit festgelegten Parametern gibt es viele Standardeinstellungen, die für die schnelle Einsatzbereitschaft von EdgeSight sorgen. In diesem Abschnitt werden die übrigen Aufgaben erläutert, die Sie nach der Installation und Erstkonfiguration ausführen können, um die vollständige Betriebsfähigkeit herzustellen. Einige dieser Aufgaben hängen von der Umgebung ab, z. B. den überwachten Systemen und ob Sie zum Authentifizieren von Benutzern den Standard-E-Mail-Authentifizierungsprovider oder Active Directory verwenden.

Konfigurieren der Authentifizierung bei Reporting Services

Zum Generieren und Anzeigen von EdgeSight-Berichten muss Microsoft SQL Server Reporting Services installiert und konfiguriert sein. Nach der Installation von EdgeSight müssen Sie die Anmeldeinformationen für die Authentifizierung des EdgeSight-Servers beim Berichtserver konfigurieren. Weitere Informationen dazu finden Sie unter "Konfigurieren der Verbindung zu Reporting Services" auf Seite 73.

Hinzufügen von Rollen

Vor dem Hinzufügen von Benutzern (also Personen, die sich auf der EdgeSight Server Console anmelden können) sollten Sie Rollen hinzufügen. Über diese werden die Aktionen festgelegt, die die einzelnen Benutzer auf der Konsole ausführen dürfen. Weitere Informationen zum Definieren von Rollen finden Sie unter "Erstellen von Benutzern und Zuweisen von Rollen" auf Seite 33.

Hinzufügen von Authentifizierungsprovidern

Wenn Sie Benutzer automatisch anhand einer Active Directory-Struktur erstellen möchten, müssen Sie einen AD-Authentifizierungsprovider hinzufügen. Stellen Sie vor dem Erstellen eines neuen Providers sicher, dass der LDAP-Pfad für den AD-Authentifizierungsprovider verfügbar ist. Weitere Informationen zum Hinzufügen eines AD-Authentifizierungsproviders finden Sie unter "Verwalten von Authentifizierungsprovidern" auf Seite 72.

Hinzufügen von Benutzern

Wenn Sie den Standard-E-Mail-Authentifizierungsprovider verwenden, können Sie mit der EdgeSight Server Console Benutzer hinzufügen und ihnen Rollen zuweisen: Weitere Informationen dazu finden Sie unter "Erstellen von Benutzern und Zuweisen von Rollen" auf Seite 33.

Anpassen der Agent- und Workerkonfigurationen

Je nach Umgebung müssen Sie u. U. Anpassungen vornehmen, welche Agent- und Workerkonfigurationen auf die Geräte in einer Abteilung angewendet werden. Standardmäßige Agent- und Workerkonfigurationen sind für Endpunkt- und XenApp-Systeme sowie Systeme mit virtuellen Desktops verfügbar. Nur wenn sichergestellt ist, dass sich die Geräte in den richtigen Abteilungen befinden und die entsprechenden Agent- und Workerkonfigurationen auf diese Abteilungen angewendet werden, ist ein effizienter Betrieb von EdgeSight Server gewährleistet. Es wird empfohlen, für einen gewissen Zeitraum die Standardkonfigurationen zu verwenden und erst dann die Konfigurationen entsprechend anzupassen, falls Probleme bei der Datenerfassung auftreten. Weitere Informationen zu Agenteigenschaften finden Sie unter "Festlegen von Agenteigenschaften" auf Seite 49. Weitere Informationen zu Workerkonfigurationen finden Sie unter "Konfigurieren, Terminieren und Ausführen von Workern" auf Seite 53.

Verwalten von Unternehmenseinstellungen

In diesem Kapitel finden Sie Richtlinien und Vorgehensweisen zum Verwalten von Konfigurationseinstellungen für Unternehmen, die auf einem Citrix EdgeSight-Server gehostet werden. Sämtliche Unternehmenseinstellungen können auf der Registerkarte **Konfiguration** über den Menübefehl **Unternehmenskonfiguration** eingesehen und geändert werden. Informationen zur globalen Serverkonfiguration finden Sie in Kapitel 3, "Überwachen des Serverstatus" .

In diesem Kapitel werden die folgenden Aufgaben beschrieben:

- Verwalten von Benutzerprofilen
- Verwalten von Unternehmenseinstellungen
- Verwalten von Abteilungen, Geräten und Gruppen
- Verwalten von Benutzergruppen
- Verwalten von Rollen
- Erstellen von Benutzern und Zuweisen von Rollen
- Verwalten des Zugriffs auf XenApp-Farmen
- Erstellen von Regeln und Aktionen für Warnungen
- Verwalten von Anwendungskategorien und Anbietern
- Verwalten von Berichten
- Verwalten von IP-Bereichen
- Verwalten von Echtzeit-Dashboard-Konfigurationen
- Festlegen von Agenteigenschaften
- Konfigurieren, Terminieren und Ausführen von Workern
- Fehlerbehebung anhand von Agentprotokolldateien

Verwalten von Benutzerprofilen

Auf dem Server ist für jeden EdgeSight Server Console-Benutzer ein Profil mit Angaben zum Namen, zum Titel und zur Kontaktaufnahme gespeichert. Diese Profile können von den Benutzern selbst bearbeitet werden. Klicken Sie auf **Eigene Einstellungen > Profil**, um das Profil zu dem Benutzernamen anzuzeigen, unter dem Sie sich bei der Konsole angemeldet haben.

Über die Seite "Benutzer" (**Unternehmenskonfiguration > Sicherheit > Benutzer**) können Sie die Profile anderer EdgeSight Server Console-Benutzer anzeigen. Weitere Informationen zum Erstellen und Verwalten von Benutzern finden Sie unter "Erstellen von Benutzern und Zuweisen von Rollen" auf Seite 33.

Verwalten von Unternehmenseinstellungen

Unternehmen sind die primäre Organisationseinheit auf einem EdgeSight-Server. Ein einzelner Server kann mehrere Unternehmen unterstützen. Wenn sich auf dem Server mehrere Unternehmen befinden, können Sie über die Dropdownliste **Unternehmen** in der rechten Ecke der Konsole zwischen den einzelnen Unternehmen wechseln. Unternehmenseinstellungen werden separat von Servereinstellungen verwaltet, sodass Serveradministratoren genau steuern können, welche Benutzer berechtigt sind, für ein konkretes Unternehmen Berichte anzuzeigen oder Einstellungen zu ändern. Wählen Sie zum Anzeigen der Unternehmenseinstellungen **Unternehmenskonfiguration > Einstellungen**.

Zeitzone und Sommerzeit

Für jedes Unternehmen auf einem EdgeSight-Server gilt eine Zeitzone. Die Zeitzone wird vom Server zum Anzeigen von Uhrzeiten in Berichten, für das Planen und Ausführen von Wartungsaufträgen und für Zeitstempel für Ereignisse, z. B. Warnungen und Upload-Zeiten, verwendet. Zur tageweisen Konsolidierung der Daten für ein Unternehmen wird die für das jeweilige Unternehmen geltende Zeitzone mit ihren Tagesgrenzen herangezogen. Dies sorgt für größere Datenkonsistenz, wenn sich die Agentcomputer in verschiedenen Zeitzonen befinden. Neben der Zeitzone können Sie auch festlegen, ob die Sommerzeit berücksichtigt werden soll.

Beim Installieren von EdgeSight muss ein erstes Unternehmen erstellt und dafür eine Zeitzoneneinstellung festgelegt werden. Bei Bedarf kann diese Zeitzoneneinstellung über die Seite "Unternehmenseinstellungen" geändert werden. Beim Erstellen neuer Unternehmen über die Konsole müssen Sie dann ebenfalls eine Zeitzone festlegen. (Weitere Informationen dazu finden Sie unter "Erstellen von Unternehmen" auf Seite 65.)

Agentregistrierungseinstellungen

Die Agentregistrierungseinstellungen steuern, wie EdgeSight-Agents sich dem Server gegenüber zu erkennen geben. (Die Kommunikation mit dem Server geht in der Regel von den Agents aus, es sei denn, es werden explizit Agentdaten angefordert. Dies kann z. B. der Fall sein, wenn über die Konsole ein Echtzeitbericht angezeigt wird.) Sie können die einzelnen Einstellungen über die Menüs aktivieren und deaktivieren. Klicken Sie dann auf **Änderungen speichern**, damit die neuen Einstellungen wirksam werden. Es wird empfohlen, alle Agentregistrierungseinstellungen zu aktivieren. Sie können die Agentregistrierung, die Abteilungserstellung und das Duplizieren von Instanzen der EdgeSight-Software überlassen und so Zeit und Mühe sparen, die andernfalls für das manuelle Auflösen dieser Ereignisse aufgewendet werden müsste. In der folgenden Tabelle wird beschrieben, wie jede Einstellung sich auf die Agentregistrierung auswirkt.

Registrierungseinstellung	Wirkung
Agents automatisch registrieren	Wenn ein Agent eine Verbindung mit einem Server herstellt, werden Informationen zur Unternehmens- und Abteilungskonfiguration übermittelt. Stimmen diese Informationen mit einem auf dem Server definierten vorhandenen Unternehmen überein und ist diese Einstellung aktiviert, wird der Agent dem Unternehmen zugewiesen. Andernfalls ist der Agent eine nicht verwaltete Instanz und wird nur auf der Seite "Nicht verwaltete Geräte" angezeigt. (Weitere Informationen zum Verschieben nicht verwalteter Geräte in ein Unternehmen oder eine Abteilung finden Sie unter "Umgang mit nicht verwalteten Geräten" auf Seite 78.)
Abteilungen automatisch erstellen	Wenn ein Agent eine Verbindung mit einem Server herstellt, werden Unternehmens- und Abteilungsinformationen übermittelt. Wenn die Abteilung nicht vorhanden ist, wird sie erstellt, wenn diese Einstellung aktiviert ist. Wenn die Einstellung nicht aktiviert ist, wird das Gerät in die Stammabteilung des Unternehmens gestellt. (Weitere Informationen zu Abteilungen finden Sie unter "Verwalten von Abteilungen" auf Seite 28.)
Doppelte Instanzen zusammenführen	Wenn diese Einstellung aktiviert ist und eine EdgeSight-Agentdatenbank beschädigt wird, wird der Computer im Rahmen des Reparaturvorgangs mit seinen Verlaufsdaten auf dem Server abgeglichen. Wenn diese Einstellung deaktiviert ist, wird im System ein doppelter Datensatz des Geräts erstellt. Ist dies der Fall, erscheint auf der Seite "Nachrichten" eine Nachricht der folgenden Art:# `EdgeSight - Neue Instanz (DUPLIKAT) - Computer: '`*`Sysname`*`' Domäne: '`*`Domänenname`*`' #` Die Zusammenführung der doppelten Instanzen erfolgt anhand einer internen Kennung (GUID) und nicht anhand des Computernamens.

Verwalten von Abteilungen, Geräten und Gruppen

Unternehmen untergliedern sich in Abteilungen. Abteilungen sind in einer hierarchischen Struktur organisiert mit einer Standardstammabteilung (Alle) und gerätspezifischen Unterabteilungen (XenApp-Farmen, XenDesktop-Farmen und Endpunkte), die bei der Installation erstellt werden. Endpunktunterabteilungen können automatisch erstellt werden, wenn Agenten beim Server registriert werden, oder sie können von Benutzern mit Administratorprivilegien manuell erstellt werden. Jeder Abteilung ist ein Satz Geräte zugeordnet (Systeme, die EdgeSight-Agents ausführen).

Zusätzlich zur Strukturierung nach Abteilung können Sie Geräte auch nach benutzerdefinierten Gruppen organisieren. Eine Gruppe ist eine vom Benutzer zusammengestellte Sammlung von Geräten. Die Mitgliedschaft in einer Gruppe kann sich nach den verknüpften Abteilungen, den Gerätemerkmalen oder Abfragen richten.

Verwalten von Abteilungen

Die Stammabteilung (die standardmäßig die Bezeichnung "Alle" trägt) und die Unterabteilungen "XenApp-Farmen", "XenDesktop-Farmen" und "Endpunkte" werden bei der Installation von EdgeSight erstellt. Diese Standardabteilungen können nicht gelöscht werden. Die Stammabteilung verwendet für Agenteigenschaften und Agentworker die Endpunkt-Standardkonfiguration. Warnungsregeln müssen explizit mit der Stammabteilung verbunden werden. Die Struktur der Unterabteilung für XenApp-Farmen wird durch die XenApp-Farmstruktur bestimmt und die Struktur der XenDesktop-Farm wird vom Desktop Delivery Controller bestimmt. Diese Unterabteilungen können nicht mit der EdgeSight Server Console geändert werden.

Endpunkt-Unterabteilungen können, auf der Grundlage der Informationen von den Agents, die sich beim Server registrieren, automatisch erstellt werden. Wenn ein Endpunktagent eine Verbindung zu einem Server herstellt, übergibt er Unternehmens- und Abteilungsinformationen. Wenn die Abteilung nicht existiert, wird sie erstellt, sofern die Einstellung **Abteilungen automatisch erstellen** aktiviert ist (siehe dazu "Agentregistrierungseinstellungen" auf Seite 27). Wenn die Einstellung nicht aktiviert ist, wird das Gerät in die Stammabteilung des Unternehmens gestellt.

Wenn Sie ein Upgrade auf EdgeSight 5.0 vornehmen, werden alle Geräte, einschließlich XenApp-Server, in die Unterabteilung für Endpunkte platziert.

Über die Seite "Abteilung" können Sie Endpunkt-Unterabteilungen erstellen, bearbeiten und löschen sowie Warnungsregeln und Konfigurationseinstellungen mit Geräten in der Abteilung verknüpfen. Warnungsregeln, Workerkonfigurationen und Agenteigenschaften können zwar jederzeit erstellt oder bearbeitet werden, verwendet werden sie aber erst, wenn sie explizit mit Abteilungen verknüpft sind. Ausführliche Anweisungen zum Erstellen und Bearbeiten von Abteilungen und zum Zuweisen von Regeln und Konfigurationen zu Abteilungen finden Sie in der Onlinehilfe der Konsole unter dem Stichwort "Abteilungen".

Verwalten von Geräten

Die auf der Seite "Geräte" angezeigten Geräte stehen für Systeme, auf denen EdgeSight-Agents ausgeführt werden und die sich erfolgreich beim Server registriert haben. Geräte können XenApp-Server, Desktops, Laptops oder Terminalserver sein. Es können physikalische oder virtuelle Maschinen sein. Wenn Sie die Standardeigenschaften für die Agentregistrierung gewählt haben, die die automatische Agentregistrierung und die Abteilungshierarchieerstellung ermöglichen, werden in der Liste der Geräte automatisch alle Agents eingetragen, die für die Kommunikation mit dem Server konfiguriert sind. Wenn sich ein Agent, der auf einem Gerät ausgeführt wird, beim Server registriert hat, können Sie das Gerät bei Bedarf in eine andere Abteilung verschieben. (Weitere Informationen zur Agentregistrierung finden Sie unter "Agentregistrierungseinstellungen" auf Seite 27.)

Der Gerätename, die Domäne und der Zeitpunkt des letzten Uploads für das Gerät werden immer angezeigt. Die übrigen Geräteinformationen können über die Dropdownliste **Anzeigen** ausgewählt werden. In der Onlinehilfe finden Sie eine vollständige Liste der verfügbaren Informationen. Beachten Sie, dass der Zeitpunkt des letzten Uploads, der in der Tabelle "Geräte" angezeigt wird, der Zeitpunkt ist, zu dem der Server zuletzt Nutzdaten von diesem Gerät verarbeitet hat. Es handelt sich dabei um eine nützliche Angabe, der entnommen werden kann, dass die Agents ordnungsgemäß Daten auf den Server hochladen.

Wenn ein bestimmtes Gerät in der Liste nicht angezeigt wird, kann dies auf ein Problem mit der Zuordnung zum Unternehmen/zur Abteilung hindeuten. Wählen Sie **Serverkonfiguration > Nicht verwaltete Geräte**, um eine Liste der Geräte anzuzeigen, die sich zwar beim Server registriert haben, die aber keinem Unternehmen oder keiner Abteilung zugeordnet sind. Weitere Informationen zum Umgang mit nicht verwalteten Geräten finden Sie unter "Umgang mit nicht verwalteten Geräten" auf Seite 78.

Erstellen und Verwenden benutzerdefinierter Gerätegruppen

Sie können in EdgeSight Server benutzerdefinierte Gerätegruppen erstellen. Gruppen sind Zusammenstellungen von Geräten nach Abteilung, einem ausgewählten Satz Einzelgeräte, SQL-Abfragen oder einer Kombination dieser Kriterien. Bei der Installation von EdgeSight werden eine Reihe häufig verwendeter Benutzergruppen bereitgestellt, wie z. B. "Citrix XenApp" und "Alle Windows Server 2003". Gruppen können mit den folgenden Kriterien (auch Kombinationen daraus) definiert werden:

- Alle Geräte in einer oder mehreren Abteilungen
- Ausgewählter Satz Einzelgeräte innerhalb einer Abteilung oder über Abteilungsgrenzen hinweg
- Ausgewählter Satz Einzelgeräte, die aus der Gruppe *ausgeschlossen* werden sollen
- Satz Einzelgeräte, die mit einer SQL-Abfrage aus der EdgeSight-Datenbank ausgewählt wurden

Durch das Erstellen von Gruppen können Sie Daten anhand spezifischer Geräteeigenschaften isolieren und anzeigen und damit abteilungsübergreifende Systemverwaltungsprobleme besser lösen. Bei den folgenden Beispielen handelt es sich um Situationen, in denen sich die Verwendung benutzerdefinierter Gruppen anbietet:

- Sie werden gebeten einzuschätzen, welche Leistungsverbesserungen durch den Umstieg auf ein neues Betriebssystem erzielt werden könnten. Erstellen Sie dazu benutzerdefinierte Gerätegruppen: eine Gruppe mit Geräten, die das aktuelle Betriebssystem verwenden, und eine Gruppe mit Geräten, die das neue Betriebssystem verwenden. Vergleichen Sie dann die Leistung der beiden Gruppen über einen gewissen Zeitraum hinweg.
- Sie werden gebeten, die Effektivität eines Software-Patches zu ermitteln, bevor dieser unternehmensweit bereitgestellt wird. Erstellen Sie dazu benutzerdefinierte Gerätegruppen: eine Gruppe mit installiertem Patch und eine Gruppe ohne den Patch. Vergleichen Sie dann die Leistung und Verfügbarkeit der entsprechenden Anwendung über einen gewissen Zeitraum hinweg.
- Sie werden gebeten, eine Gerätegruppe genau zu überwachen, da für diese Gruppe Hardwareprobleme bekannt sind. Diese Geräte befinden sich in unterschiedlichen Abteilungen. Erstellen Sie dazu eine benutzerdefinierte Gruppe mit den Zielsystemen und filtern Sie die eingehenden Warnungen anhand dieser Gruppe.

Gruppen haben die folgenden Attribute:

- *Name*: Eindeutiger Name der Gruppe. Der Name sollte so aussagekräftig sein, dass ein Konsolenbenutzer in einer Dropdownliste problemlos die richtige Gruppe auswählen kann.
- *Ablauffrist*: Festgelegter Zeitraum, nach dem die Gruppe abläuft und gelöscht wird. Diese Funktion erlaubt es, Gruppen für kurzfristige Projekte mit begrenzter Dauer zu erstellen (Beispiel: Gruppe für die Beurteilung einer Software). Gruppen können auch so erstellt werden, dass sie nie ablaufen. Wenn eine Gruppe abläuft, wird vorab kein expliziter Hinweis auf das nahende Ablaufdatum gesendet.
- *Aktualisierungsrate*: Festgelegtes Intervall, nach dessen Ablauf der Gerätecache für die Gruppe aktualisiert wird. Durch die Aktualisierung des Gerätecaches wird sichergestellt, dass Geräte, die die Kriterien für die Gruppenmitgliedschaft erfüllen, erkannt und der Gruppe hinzugefügt werden.
- *Öffentlich/Privat*: Gruppen können öffentlich (alle Konsolenbenutzer mit der Rolle "Administrator" können sie verwenden) oder privat sein (nur der Benutzer, der die Gruppe erstellt hat, kann sie verwenden). Die Einrichtung privater Gruppen für ausgewählte Konsolenbenutzer ist derzeit nicht möglich.
- *Mitgliedstyp*: Gruppenzuordnungen können anhand einer oder mehrerer der folgenden Kriterien erfolgen: Abteilung, ausgewählter Satz Geräte oder SQL-Abfrage. Abteilungen können als einzelne Abteilung oder als Abteilungsstruktur mit der ausgewählten Abteilung und allen Unterabteilungen enthalten sein. Ein Satz Geräte kann aus einer Liste vorhandener Geräte ausgewählt oder aus einer CSV-Datei importiert werden. Das Erstellen von Gruppen anhand einer SQL-Abfrage ist eine erweiterte Funktion, die wahrscheinlich nur dort erforderlich ist, wo ein Satz Geräte benötigt wird, die nur sehr eng gesteckte Kriterien erfüllen. In diesen Fällen müssen Sie Datenbanktools verwenden, um die Datenbankstruktur anzuzeigen.

Hinweis: Es hat sich bewährt, den Ablaufzeitraum auf einen Wert zu setzen, der die Laufzeit der damit verbundenen Aufgabe widerspiegelt. Wenn Sie z. B. einen Patch beurteilen und 3 Wochen lang Daten erfassen müssen, wählen Sie als Ablaufzeitraum 1 Monat. Wenn Sie mehr Zeit zum Erfassen von Daten brauchen, können Sie den Ablaufzeitraum jederzeit ändern. Das Festlegen realistischer Ablaufzeiträume hilft, die Liste der Gruppen für Sie und andere Benutzer verwaltbar zu halten (wenn die Gruppen öffentlich sind). Da der Gerätecache der

Gruppe in regelmäßigen Abständen aktualisiert wird, hilft das Festlegen von Ablaufzeiträumen auch, Systemressourcen vernünftig zu verwalten.

Ausführliche Anweisungen zum Erstellen von benutzerdefinierten Gruppen finden Sie in der Onlinehilfe unter dem Stichwort "Gruppen".

Verwalten von Benutzergruppen

Sie können nicht nur Gerätegruppen, sondern auch Benutzergruppen erstellen. Die EdgeSight-Funktionen zur Gruppenerstellung erlauben es Ihnen, Gruppen von Benutzern zusammenzustellen, indem Sie sie nach Benutzername, IP-Adresse oder IP-Bereich auswählen oder indem Sie eine SQL-Abfrage der EdgeSight-Datenbank durchführen. Die Benutzer können XenApp-, XenDesktop- oder Endpunktbenutzer sein. Viele Berichte mit Daten zum Benutzererlebnis können nach Benutzergruppen gefiltert werden, sodass Sie die Systemleistung für eine Gruppe von Benutzern mit spezifischen Eigenschaften überwachen können.

Wählen Sie zum Verwalten von Benutzergruppen **Unternehmenskonfiguration > Benutzergruppen**. Für Benutzergruppen können Sie festlegen, wie sie heißen sollen, ob sie öffentlich oder privat sein sollen und wer zur Gruppe gehören soll. Benutzergruppen können öffentlich (alle Konsolenbenutzer mit der Rolle "Administrator" können sie verwenden) oder privat sein (nur der Benutzer, der die Gruppe erstellt hat, kann sie verwenden).

Die Auswahl der Gruppenmitglieder kann aus einer Liste von Benutzern (anhand ihres Benutzernamens oder ihrer IP-Adresse), anhand eines Bereiches von IP-Adressen oder durch eine SQL-Abfrage aus der EdgeSight-Datenbank erfolgen. Beachten Sie, dass beim Aktualisieren eines Benutzergruppencache die Abfrage erneut ausgeführt und neue Benutzer, auf die die Abfrage zutrifft, der Benutzergruppe hinzugefügt werden, wenn die Gruppenmitgliedschaft durch eine Abfrage gesteuert wird. Dadurch wird die Wartung abfragebasierter Gruppen deutlich vereinfacht. Ausführliche Anweisungen zum Erstellen von Benutzergruppen finden Sie in der Onlinehilfe unter dem Stichwort "Benutzergruppen".

Verwalten von Rollen

Beim Konfigurieren von Benutzern auf einem Citrix EdgeSight-Server werden ihnen Rollen zugewiesen. Rollen definieren einen Satz Berechtigungen, mit denen gesteuert wird, welche Operationen ein Benutzer ausführen kann. Ein EdgeSight-Administrator kann neue Rollen definieren und vorhandene benutzerdefinierte Rollen bearbeiten. Es gibt zwei systemdefinierte Rollen, die sich nicht bearbeiten lassen: Administrator und Berichts-Viewer. Die Administratorrolle verfügt über alle Berechtigungen und der Berichts-Viewer verfügt über eingeschränkte Berechtigungen, mit denen er alle EdgeSight-Berichte anzeigen kann. Zum Erstellen von Rollen gehört die Auswahl der mit der Rolle verknüpften Berechtigungen. Sie können die Rollen optional auch vorhandenen Benutzern zuweisen. Weitere Informationen zur Erstellung von Rollen finden Sie in der Onlinehilfe im Abschnitt "Hinzufügen neuer Rollen".

Erstellen von Benutzern und Zuweisen von Rollen

Ein Benutzer ist eine Person (oder eine Gruppe von Personen), für die in der EdgeSight Server Console ein Konto erstellt wurde. Bei der Erstkonfiguration des Servers wird ein Superuser-Konto erstellt. Dieses Konto hat Zugriff auf alle Unternehmen, die auf dem Server gehostet werden, und kann andere Benutzer erstellen. Der Superuser kann ein Konto für einen oder mehrere Administratoren eines Unternehmens erstellen und die Administratoren wiederum können nach Bedarf weitere Benutzerkonten erstellen. Das Erstellen und Verwalten von Benutzern erfolgt auf der Seite "Benutzer" (**Unternehmenskonfiguration > Sicherheit > Benutzer**). Nachdem Sie einen Benutzer erstellt haben, erhält der Benutzer eine E-Mail mit Anweisungen zum Anmelden und mit einem temporären Kennwort. Ausführliche Anweisungen zum Erstellen von Benutzern finden Sie in der Onlinehilfe unter dem Stichwort "Benutzer".

Der Benutzerzugriff auf die EdgeSight Server Console wird über die Authentifizierung bei der Anmeldung gesteuert. Ob der einzelne Benutzer dann Daten anzeigen und bearbeiten sowie Verwaltungsaufgaben ausführen kann, richtet sich nach einem System von Rollen und Berechtigungen.

Benutzeranmeldungen werden entweder durch den integrierten EdgeSight-Provider (anhand von E-Mail-Adresse und Kennwort des Benutzers) oder durch Active Directory (AD) authentifiziert. (Informationen zum Erstellen eines AD-Authentifizierungsproviders finden Sie unter "Verwalten von Authentifizierungsprovidern" auf Seite 72 und in der Onlinehilfe unter dem Stichwort "Authentifizierung".)

Neuen Benutzern kann eine der vordefinierten Rollen ("Administrator" oder "Berichts-Viewer") oder eine zuvor erstellte benutzerdefinierte Rolle zugewiesen werden. Für jede Rolle gilt ein Satz Berechtigungen. Beim Zuweisen einer Rolle zu einem Benutzer erhält dieser Benutzer automatisch die zugehörigen Berechtigungen. Ausführliche Anweisungen zum Erstellen von Rollen finden Sie in der Onlinehilfe unter dem Stichwort "Rollen".

Wenn Sie alle Berechtigungen anzeigen möchten, die über eine Rolle zugewiesen werden können, wählen Sie **Unternehmenskonfiguration > Sicherheit > Rollen**, klicken Sie auf das Informationssymbol für die Rolle "Administrator" und wählen Sie in der Detailansicht die Registerkarte **Berechtigungen** aus.

Beachten Sie, dass die Berechtigung "Servereinstellungen verwalten" nicht in der Liste erscheint. Diese Berechtigung muss beim Erstellen oder Bearbeiten eines Benutzers explizit gewährt werden und kann nicht mit einer Rolle zugewiesen werden. Im Unterschied zu anderen Berechtigungen, die es Benutzern erlauben, Operationen auf Unternehmensebene auszuführen, erhält der Benutzer mit dieser Berechtigung die Möglichkeit, serverweite Einstellungen anzuzeigen.

Verwalten des Zugriffs auf XenApp-Farmen

Auf der Seite "Farm-Authentifizierung" können Standardanmeldeinformationen für den Zugriff auf XenApp-Farmen erstellt und gepflegt werden. Die Anmeldeinformationen setzen sich aus einem Farmnamen, einem Benutzernamen, einem Kennwort und dem Domänennamen zusammen. Die Anmeldeinformationen werden beim direkten Abfragen von Farmen beim Suchen nach aktiven Sitzungen verwendet. (Auf diesen Bericht kann über die Registerkarte "Fehlerbehebung" zugegriffen werden.) Um nach Benutzersitzungen zu suchen und diesen Bericht anzuzeigen, müssen Sie eine Abfragemethode auswählen. Für die Suche nach einer aktiven Sitzung eines bestimmten Benutzers empfiehlt sich die Methode **Eine oder mehrere Farmen direkt abfragen**. Da diese Methode das Vorhandensein von Anmeldeinformationen für die Anmeldung bei den ausgewählten Farmen voraussetzt, müssen Sie für jede Farm einen Satz Anmeldeinformationen festlegen, damit Berichte anhand dieser Abfragemethode generiert werden können. Beachten Sie, dass Anmeldeinformationen nicht für Abteilungen gespeichert werden können, die keine Geräte haben.

Erstellen von Regeln und Aktionen für Warnungen

In diesem Abschnitt werden die grundlegenden Konzepte von Echtzeitwarnungen sowie Strategien und Richtlinien für das Implementieren von Warnungen in EdgeSight vorgestellt. Ausführliche Anweisungen zum Erstellen von Echtzeitwarnungen und Aktionen finden Sie in der Onlinehilfe in den Abschnitten "Warnungsregeln" und "Warnungsaktionen".

Mit Echtzeitwarnungen können Sie essentielle Anwendungen und Geräte überwachen und, falls ein Problem auftritt, die zuständigen Personen benachrichtigen. Standardmäßig werden Warnungsdaten und -statistiken vom Agent auf dem jeweiligen Desktop erfasst und einmal täglich auf den Server hochgeladen. Wenn Sie eine Warnung explizit durch Erstellen einer Warnungsregel konfigurieren, fordern Sie eine Echtzeitbenachrichtigung an, dass eine bestimmte Warnungsbedingung eingetreten ist.

Ziel von Echtzeitwarnungen ist es, im Falle kritischer Ereignisse, die der sofortigen Aufmerksamkeit bedürfen, eine schnelle Benachrichtigung zu erreichen. Mit Warnungsregeln wird z. B. sichergestellt, dass Daten immer verfügbar sind, um sie mit der Farmüberwachung anzuzeigen. Die Farmüberwachung ermöglicht es Ihnen, eine XenApp-Farm zu durchsuchen und Echtzeitwarnungen und Systemkontext für ein oder mehrere Geräte anzuzeigen. Beim Entwickeln einer Warnungsregelstrategie sollten Sie dafür sorgen, dass Warnungsregeln nur für solche Ereignisse erstellt werden, denen eine Lösung zugeordnet ist. Echtzeitwarnungen sind *nicht* dazu gedacht, Daten zu erfassen. Agents erfassen relevante Daten unabhängig davon, ob eine Warnungsregel existiert, und für das Anzeigen von Verfügbarkeits- und Leistungsdaten steht eine breite Palette höchst aussagekräftiger Berichte zur Verfügung.

Die richtige Warnungskonfiguration spielt für eine effektive Echtzeit-Warnungsbenachrichtigung zum Zustand der verteilten Geräte und Anwendungen eine entscheidende Rolle. Eine geeignete Konfiguration versetzt Sie in die Lage, schnell herauszufinden, welche Probleme wirklich kritisch sind und sofortiger Aufmerksamkeit bedürfen und welche Probleme warten können. Voraussetzung für eine effektive Warnungskonfiguration ist das Vorhandensein einer Warnungsstrategie. Beim Entwickeln Ihrer Strategie müssen Sie Folgendes tun:

- Identifizieren, welche Anwendungen für Ihr Unternehmen oder Ihren Dienst kritisch sind: Konzentrieren Sie sich nur auf wirklich kritische Anwendungen und definieren Sie Warnungen für Probleme, die kurzfristig gelöst werden müssen.

- Identifizieren, welche Abteilungen auf ihren Systemen essentielle Anwendungen ausführen: Weisen Sie Warnungen nur den Abteilungen oder Gruppen zu, bei denen die Warnungsbedingung höchste Relevanz hat. Auf diese Weise können Sie Probleme isolieren und auf Probleme reagieren, die nur für einen bestimmten Teil Ihres Unternehmens relevant sind.

- Identifizieren, welche Warnungstypen am wichtigsten sind: Bestimmte Warnungen, wie z. B. NT-Protokollwarnungen, werden von einigen Anwendungen in großen Mengen generiert und sind normalerweise für den Endbenutzer transparent. Überprüfen Sie daher vor dem Definieren einer NT-Protokollwarnung, wie hoch das Risiko der Warnungsbedingung ist, indem Sie sich Verlaufsberichte mit Warnungen ansehen.
- Identifizieren, welche Reaktionen zur Lösung bestimmter Warnungen erforderlich sind: Eine mögliche Reaktion auf eine Warnung besteht z. B. darin, eine konkrete Abfolge von Aktionen auszuführen oder die zuständigen Personen in der entsprechenden Abteilung zu informieren. Wenn für eine Bedingung keine Reaktion identifiziert werden kann, muss für das Ereignis auch keine Echtzeitwarnung erstellt werden.
- Identifizieren, wer für das Reagieren auf eine Warnung verantwortlich ist: Legen Sie fest, wer für die einzelnen Warnungsbedingungen zuständig ist.
- Einrichten und Veröffentlichen von Richtlinien für das Erstellen von Warnungsregeln: Bestimmen Sie, wer für das Erstellen neuer Warnungsregeln zuständig ist, und definieren Sie bewährte Vorgehensweisen, wie z. B. dass aussagekräftige Namen für Warnungsregeln zu verwenden sind und dass Dopplungen bei der Erstellung von Warnungsregeln vermieden werden sollten. Benutzer, die Warnungsregeln erstellen oder bearbeiten können sollen, benötigen die Berechtigung "Warnungen verwalten".

Wenn Sie eine Warnungsstrategie aufgestellt haben, können Sie die erforderlichen Echtzeitwarnungen über die Seite "Warnungsregeln" in der EdgeSight Server Console (**Unternehmenskonfiguration > Warnungen > Regeln**) konfigurieren.

Funktionen für Warnungen

Es gibt eine Reihe von Funktionen, die Ihnen dabei helfen, Warnungsregeln für Bedingungen zu konfigurieren, bei denen unbedingt eine Warnung ausgegeben werden sollte. So können Sie die Anzahl der nicht relevanten Warnungen, die vom Agent generiert werden, verringern. Diese präzisen Warnungsregeln sollten, falls die Warnung einmal ausgegeben wird, zu einer zielgerichteten Reaktion führen. In der folgenden Liste finden Sie eine Zusammenstellung einiger entsprechender Szenarios:

- Warnungsregeln zur Leistung können anhand komplexer Parameter eingerichtet werden. So kann z. B. festgelegt werden, dass eine Warnung zur Systemleistung gesendet wird, wenn die CPU zu mehr als *x* % ausgelastet ist und auf dem Computer nur noch weniger als *y* freier Arbeitsspeicher vorhanden ist.

- Es können Regeln für Anwendungswarnungen definiert werden, um so den Unternehmensnamen des Prozesses anzugeben, von dem aus die Warnungsregeln generiert werden sollen. Wenn z. B. ein vom angegebenen Unternehmen geschriebener Prozess abstürzt, kann eine Warnung "Prozessfehler" an das unternehmensinterne Support-Team gesendet werden.
- Es können Regeln für Windows-Ereignisprotokollwarnungen festgelegt werden, um so die Anwendung und das Ereignis einzuschließen, die bzw. das das Ereignis in das Ereignisprotokoll schreibt. Wenn es z. B. zu einer Verletzung einer Gruppenrichtlinie kommt, kann eine Warnung an das für die Sicherheit zuständige Team gesendet werden.
- Beim Definieren bestimmter Warnungsregeln kann jetzt die Negationslogik (implementiert über das Kontrollkästchen **entspricht nicht**) verwendet werden. So kann z. B. festgelegt werden, dass eine Warnung, die über die Beendigung einer Anwendung informiert, nur dann gesendet wird, wenn der beendete Prozess nicht vom internen Tools-Team geschrieben wurde.

Warnungskategorien und -typen

Echtzeitwarnungen können in zwei Kategorien unterteilt werden: ereignisgesteuerte Warnungen und Abfragewarnungen. Ereignisgesteuerte Warnungen werden immer dann generiert, wenn das damit verbundene Ereignis im System auftritt, während Abfragewarnungen auf regelmäßig stattfindenden Abfragen der Agentdatenbank basieren. Im Allgemeinen werden Abfragewarnungen als Benachrichtigungen bei Leistungsproblemen einer Anwendung, eines Systems oder des Netzwerks verwendet. Eine Beschreibung der Funktionsweise von Abfragewarnungen finden Sie unter "Parameter für Stichprobenentnahme, Abfrage und erneute Warnung" auf Seite 41.

Beim Einrichten von Warnungsregeln mit dem Assistenten für Warnungsregeln werden die Warnungen je nach Ereignis- oder Bedingungstyp, mit dem sie verbunden sind, nach folgenden Typen gruppiert:

- Anwendungswarnungen
- Systemwarnungen
- Netzwerkwarnungen
- XenApp-Leistungswarnungen
- XenApp-Fehlerwarnungen
- Sitzungsleistungswarnungen

Um sicherzustellen, dass Echtzeitwarnungsdaten für XenApp- Server zur Verfügung stehen, sind folgende Warnungen vorkonfiguriert und der Unterabteilung "XenApp-Farmen" zugewiesen:

- Konfigurationsprotokollierungsdatenbank nicht verfügbar
- Fehler bei der Verbindung zum Datenspeicher der Farm
- Fehler von Systemüberwachung und -wiederherstellung bei der Wiederherstellung
- Testfehler bei Systemüberwachung- und -wiederherstellung
- IMA-Dienst reagiert nicht mehr
- Fehler bei der Verbindung zum Lizenzserver
- Anzahl der Server in einer Zone ist zu hoch
- Beschränkung der gleichzeitigen Nutzung einer veröffentlichten Anwendung
- Sitzung deaktiviert
- Fehler bei Clientverbindung zu Terminalserver
- Fehler bei der Lizenzservererkennung für Terminalserver
- Wahl des Datenkollektors für eine Zone ausgelöst
- Wahlen in Zone zu häufig

Sie können die Parameter für diese Warnungen bearbeiten. Eine Beschreibung der einzelnen Warnungsregeln und Parametergruppen finden Sie im Assistenten für die Erstellung von Warnungsregeln.

Active Application Monitoring-Warnungen

In der EdgeSight Server Console werden Echtzeitwarnungen von der Citrix Active Application Monitoring-Software angezeigt. Mit dieser Software können Sie virtuelle Benutzerskripte aufzeichnen und erstellen sowie Tests definieren. Wenn die Tests ausgeführt werden, werden auf den betroffenen XenApp-Servern virtuelle ICA-Benutzersitzungen generiert. Die Ergebnisse der Tests geben Aufschluss über Anwendungsreaktionszeiten und Verfügbarkeit.

Wichtig: Um Active Application Monitoring-Warnungen zu konfigurieren, muss der EdgeSight für XenApp Agent 5.0 im erweiterten Modus ausgeführt werden.

Die Active Application Monitoring-Warnungsregeln lauten folgendermaßen:

- Die Warnung "Anwendungsreaktionsfehler" wird generiert, wenn eine überwachte Transaktion fehlschlägt.
- Die Warnung "Anwendungsreaktionszeit" wird generiert, wenn eine überwachte Transaktion den festgelegten Schwellenwert überschreitet.

Diese Warnungen fallen unter die XenApp-Leistungswarnungen. Weitere Informationen zum Installieren der Software finden Sie in der *Citrix EdgeSight-Installationsdokumentation*. Weitere Informationen zum Erstellen und Starten von Tests finden Sie in der Onlinehilfe der Active Application Monitoring-Software.

Hinweise zu spezifischen Warnungen

Die folgenden Informationen zu spezifischen Warnungen sollen Ihnen helfen, besser zu verstehen, unter welchen Bedingungen diese Art von Warnungen ausgelöst wird.

- Warnung "Neuer Prozess": Diese Warnung wird nur für Prozesse ausgegeben, die zum ersten Mal verwendet werden, nachdem die unter "Kulanzzeitraum für neuen Prozess" angegebene Zeitspanne abgelaufen ist. Der Kulanzzeitraum wird in den Agenteigenschaften festgelegt (weitere Informationen dazu finden Sie unter "Festlegen von Agenteigenschaften" auf Seite 49). Der Standardkulanzzeitraum auf XenApp-Agents beträgt z. B. 7 Tage. Wenn Sie einen Agent installieren und dann einen Prozess starten, zeichnet der Agent dies als einen Prozess, nicht aber als einen neuen Prozess auf, da die Agentdatenbank weniger als 7 Tage alt ist. Nach Ablauf dieser 7 Tage löst jeder neue Prozess (also alle Prozesse, die nicht bereits in der Agentdatenbank vorhanden sind) eine Warnung aus, sobald er ausgeführt wird. Auf diese Weise wird verhindert, dass nach dem Installieren eines Agents viele Warnungen auf einmal ausgegeben werden. Beachten Sie, dass sich der Kulanzzeitraum auf das Alter der Agentdatenbank und nicht das Datum der Erstinstallation des Agents bezieht. Wenn eine Agentdatenbank aus irgendeinem Grund neu erstellt wird, wird der Kulanzzeitraum zurückgesetzt.
- Warnung "Der Prozess reagiert nicht": Diese Art von Warnung entspricht den in Berichten angezeigten "reagiert nicht"-Warnungen. Die EdgeSight-Software verwendet die Windows-API (den "IsHangAppWindow"-Aufruf), um zu ermitteln, ob eine Anwendung nicht reagiert. Eine Anwendung gilt dann als nicht reagierend, wenn sie nicht auf eine Eingabe wartet, sich nicht im Startprozess befindet und nicht innerhalb des internen Timeout-Zeitraums von 5000 Millisekunden (5 Sekunden) die "PeekMessage"-Funktion aufgerufen hat.

- Warnungen "Prozessausfall" und "Prozess-Snapshot": Diese Art von Warnungen kann Absturzberichte generieren, wenn die auf dem verwalteten Gerät vorhandenen Bedingungen die Erfassung von Absturzdaten zulassen. Mitunter ist das System aber nicht in der Lage, die Datenerfassung zu unterstützen. Bei Prozessausfallwarnungen und den daraus entstehenden Absturzberichten müssen Sie folgende Faktoren beachten:
  - Wenn eine Absturzdatei nicht geschrieben werden kann, wird eine entsprechende Meldung in der Datei zcrash_loader aufgezeichnet. Gehen Sie zu **Serverstatus > Server Script Host**, suchen Sie es_zcrash_loader, klicken Sie auf das Menüsymbol und wählen Sie **Protokoll anzeigen**.
  - Wie alt ist der Absturzbericht? Die Optimierung von Absturzberichten unterscheidet sich von der Datenbankoptimireung und die Dauer, wie lange Absturzberichte aufbewahrt werden, wird von der Einstellung "Max. Anzahl der Tage" gesteuert. Gehen Sie zu **Serverkonfiguration > Einstellungen** und wählen Sie die Registerkarte **Absturzverarbeitung**.
  - Wie viele Protokolle können maximal gesammelt werden und wie viel Speicherpletz wird Absturzberichten zugewiesen? Siehe **"Serverkonfiguration" > "Einstellungen"**.) Bei Überschreiten entweder der maximalen Anzahl von Absturzprotokollen oder des maximalen Speicherplatzes wird die Anwendungsabsturzverarbeitung deaktiviert, bis der Grenzwert erhöht wird. Es gibt keine Vorgänge zum Zurücksetzen, um vorhandene Nutzdaten zu entfernen.
- "Fehler bei der einzelnen Nutzung einer veröffentlichten Anwendung" und "Beschränkung der gleichzeitigen Nutzung einer veröffentlichten Anwendung": Wenn Sie die Protokollierung von Verbindungssteuerungsereignissen auf dem XenApp-Server aktivieren möchten, muss die Einstellung **Verweigerungen aufgrund von Limitüberschreitungen protokollieren** aktiviert sein, damit SMA-Warnungen ausgelöst werden. Weitere Informationen zum Konfigurieren von Verbindungssteuerungsereignissen finden Sie in der *Citrix XenApp-Administratordokumentation*.

Parameter für Stichprobenentnahme, Abfrage und erneute Warnung

Bei der *Stichprobenerfassung* werden in regelmäßigen Abständen Daten vom überwachten System erfasst. Zu *Abfragen* kommt es, wenn der Agent eine Abfrage der Datenbank ausführt, um die Parameter der Warnungsregel mit den erfassten Daten zu vergleichen.

Jede Regel für eine abfragebasierte Warnung umfasst die folgenden Parameter:

- Prozentsatz der benötigten Stichproben
- Abfrageintervall
- Erneut warnen

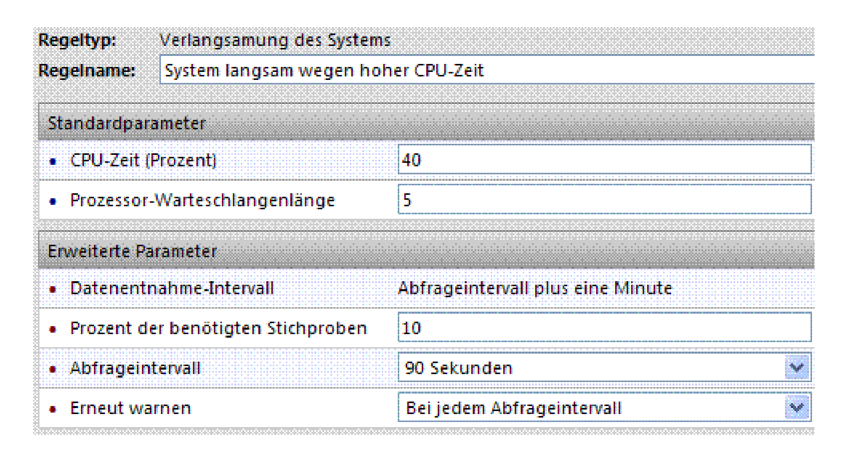
Die meisten Regeln für abgefragte Warnungen beinhalten auch ein nicht änderbares Datenentnahmeintervall, das gewöhnlich auf das Abfrageintervall plus eine Minute festgelegt ist.

Diese Parameter ermöglichen Ihnen die Optimierung der Häufigkeit, mit der Warnungen eines bestimmten Typs ausgelöst werden können. Die Stichprobenentnahme wird je nach Warnungstyp bis zu alle 5 Sekunden ausgeführt. Bei der Stichprobenentnahme werden die erforderlichen Daten für den Warnungstyp gesammelt. Beim Abfragen werden die gesammelten Daten mit in der Warnungsregel angegebenen Bedingungen verglichen. Der Abfrageintervallwert bestimmt, wie oft eine Abfrage erfolgt. Der Prozentsatz erforderlicher Stichproben bestimmt, welcher Prozentsatz der gesammelten Stichproben über dem Schwellenwert liegen muss (entweder höher oder niedriger, abhängig vom Warnungstyp), bevor eine Warnung ausgelöst wird. Wenn die durch die Warnungsregel definierte Warnung bereits innerhalb des Zeitraums für erneutes Warnen ausgelöst wurde, wird keine weitere Warnung generiert, bis der Zeitraum abgelaufen ist und der Warnungszustand erneut auftritt. Das Datenentnahmeintervall gibt an, aus welchem Zeitraum in der Vergangenheit Stichproben in Abfragen einbezogen werden sollen.

Wichtig: Das Standardabfrageintervall wurde so gewählt, dass Warnungen zeitnah ausgegeben werden, ohne dass Abfragen der Datenbank negative Auswirkungen haben. Das Verringern des Abfrageintervalls (Erhöhen der Häufigkeit, mit der Abfragen ausgeführt werden) kann die Systemleistung beeinträchtigen und sollte mit Bedacht erfolgen.

Beispiel für eine Abfragewarnung

Die folgende Abbildung zeigt eine Warnungsregel, mit der Verlangsamungen des Systems aufgrund einer hohen CPU-Auslastung erkannt werden sollen.



Die Warnung funktioniert wie folgt:

- Die EdgeSight Agent-Software erfasst in Stichproben die Belastung der CPU. In diesem Beispiel wird davon ausgegangen, dass die Stichprobenerfassung alle 5 Sekunden erfolgt.
- Alle 90 Sekunden fragt die Software die stichprobenartig erfassten Daten ab, um festzustellen, ob in mindestens 10 % der Gesamtanzahl der Stichproben die CPU mehr als 40 % genutzt wurde. Da das Datenentnahme-Intervall dem Abfrageintervall (90 Sekunden) plus eine Minute (60 Sekunden) entspricht, werden die Stichproben der letzten 150 Sekunden berücksichtigt. In dieser Zeit wurden 30 Stichproben zusammengetragen. Wenn bei mindestens 3 der 30 Stichproben die CPU zu mehr als 40 % genutzt wurde, wird eine Warnung generiert.
- Für den Parameter "Erneut warnen" ist die Einstellung **Bei jedem Abfrageintervall** festgelegt. Wenn also der Prozentsatz der CPU-Zeit den Schwellenwert in den Daten überschreitet, die bei der nächsten Abfrage erfasst werden, wird eine weitere Warnung generiert.

Wann sollte eine Regel für eine Echtzeitwarnung konfiguriert werden?

Es ist nicht erforderlich, bestimmte Warnungstypen zu konfigurieren, damit der EdgeSight-Agent Daten zu den Bedingungen erfasst, die die Warnung auslösen würden. Eine Warnungsregel sollten Sie daher nur konfigurieren, wenn Sie in der Lage sind, innerhalb weniger Stunden auf die Warnung zu reagieren. Wenn auf die Warnungsbedingung innerhalb von ein paar Stunden nach dem Generieren der Warnung nicht angemessen reagiert wurde, sollte mithilfe eines Verlaufsberichts herausgefunden werden, ob ein Ereignis größerer Tragweite stattgefunden hat. Wenn Sie zu viele Warnungsregeln erstellen, kann dies die Wirksamkeit der Überwachungstools senken, z. B. wenn die Farmüberwachung mit Warnungen überflutet wird, wodurch es schwieriger wird, wirklich schwerwiegende Ereignisse zu erkennen.

Auswirkung von Echtzeitwarnungen auf die Leistung

Unabhängig davon, welche Art von Regel für die jeweilige Warnung konfiguriert wurde, ist damit immer ein gewisser Verarbeitungsoverhead verbunden. So muss der Agent mindestens bestimmen, ob die Warnung generiert werden muss, und wenn diese Frage bejaht wird, muss er die Warnung an den Server senden. Mitunter muss der Agent eine SQL-Abfrage der Datenbank durchführen, um festzustellen, ob warnungsbedürftige Bedingungen vorliegen, und wenn die Bedingungen zu breitgefächert sind, muss der Agent große Datensätze verarbeiten, um die Warnungen zu generieren und diese anschließend an den Server zu senden.

Da jede konfigurierte Warnungsregel für einen Agent mit Verarbeitungsoverhead verbunden ist und diese Verarbeitung auch dann erfolgen kann, wenn der Endbenutzer versucht, eine wichtige Aufgabe auszuführen, sollten Warnungsregeln nur konfiguriert werden, wenn sie zielorientiert sind und entsprechende Maßnahmen nach sich ziehen können. Wenn es Bedenken hinsichtlich der Gesamtauswirkungen des Agents auf das System gibt und für den Agent eine große Zahl von Warnungsregeln definiert wurde, sollten Sie die definierten Regeln eventuell einer nochmaligen Prüfung unterziehen, um sicherzustellen, dass das Definieren einer Regel für eine Echtzeitwarnung das richtige Mittel ist oder ob ein Verlaufsbericht nicht angemessener wäre. Die folgende Liste enthält einige Situationen, in denen Warnungsregeln die Systemgeschwindigkeit für die Endbenutzer beeinträchtigen können.

- Es sind mehr als drei oder vier Warnungen zur Anwendungs- oder Netzwerkleistung definiert.
- Es sind Warnungen zur Prozess- oder Netzwerkleistung definiert, die bereits unter normalen Bedingungen, z. B. schon bei einer CPU-Auslastung von über 5 %, ausgelöst werden.
- Es sind Warnungen zur Prozess- oder Netzwerkleistung für sehr komplexe Bedingungen definiert (weil z. B. Werte für mehr als zwei oder drei Leistungsschwellenwerte eingegeben wurden). In diesen Fällen könnten die SQL-Abfragen, die der Agent ausführt, um festzustellen, ob eine warnungsbedürftige Bedingung vorliegt, zum Verbrauch signifikanter Datenbankzyklen führen.
- Für Warnungen zur Prozess- oder Netzwerkleistung ist der Parameter "entspricht nicht" definiert.
- Für Warnungen zur Prozess- oder Netzwerkleistung sind mehrere textbezogene "entspricht"- oder "entspricht nicht"-Operationen definiert.
- Es sind Regeln für Leistungswarnungen definiert, die nie zu einer Ausgabe einer Warnung führen (weil z. B. eine Warnung zur Prozessleistung für eine Anwendung eingerichtet wurde, deren Ausführung durch eine Gruppenrichtlinie blockiert wird).

Wann zeigt der Server eine Echtzeitwarnung an?

Echtzeitereignisse werden erst erstellt, wenn folgende Bedingungen erfüllt sind:

- Warnungsregeln sind erstellt und einer Abteilung zugewiesen
- Geräte haben den Init-Worker oder den Worker für die Konfigurationsüberprüfung ausgeführt
- Die Bedingung oder das Ereignis, die/das in der Warnungsregel festgelegt wurde, ist aufgetreten

Hinweis: Beachten Sie, dass XenApp-Warnungsregeln vorkonfiguriert sind und wie unter "Warnungskategorien und -typen" auf Seite 37 beschrieben der Abteilung XenApp-Farmen zugewiesen sind.

Warnungen werden unabhängig von ihrem Typ erst dann an den Server gesendet, wenn der Agent seine Startsequenz abgeschlossen hat. Dies kann einige Minuten dauern. Die Init- und Konfigurationsüberprüfung-Worker werden nach Abschluss der Startsequenz ausgeführt und die Ausführung der Worker findet über mehrere Minuten statt. Wenn eine Warnung generiert wurde, wird sie mit anderen Warnungen zusammengestellt, um sie an den Server zu übermitteln. Warnungen werden minutenweise gesammelt und dann an den Server gesendet, sofern eine Verbindung zum Netzwerk besteht. Wenn keine Verbindung zum Netzwerk vorhanden ist oder wenn der Agent beendet wird, bevor die Warnungen gesendet werden konnten, werden die in der Warteschlange befindlichen Warnungen nicht vom Server empfangen und die Warnungen werden auch nicht erneut gesendet (für Echtzeitwarnungen gibt es keine Garantie, dass sie vom Server empfangen werden). Auch wenn diese Warnungen nicht als Echtzeitwarnungen an den Server gesendet wurden, weil der Agent das Konfigurieren von Echtzeitwarnungen zum Zweck der Datenerfassung nicht verlangt, werden die Warnungsbedingungen dennoch erfasst und können nach einem Datenupload in den Verlaufsberichten angezeigt werden. Diese nicht gesendeten Warnungen erscheinen auch in den Echtzeitwarnungsberichten, die Daten direkt aus der Agentdatenbank enthalten.

Verwalten von Warnungsaktionen

Auf der Seite "Warnungsaktionen" (**Unternehmenskonfiguration > Warnungen > Aktionen**) können Sie eine Warnungsaktion konfigurieren, die ausgeführt wird, wenn eine bestimmte Warnungsbedingung eintritt. Mit Warnugnsaktionen können Sie folgende Aktionen ausführen:

- Senden von E-Mail-Nachrichten.
- Generieren von SNMP-Traps.
- Starten von externen ausführbaren Prozessen auf dem EdgeSight-Server.
- Weiterleiten von Warnungsdaten für Microsoft System Center Operation Manager (SCOM). Weitere Informationen zur Integration von EdgeSight-Warnungsaktionen mit SCOM finden Sie in Kapitel 5, "Integration von EdgeSight mit Microsoft System Center Operations Manager" .

Jede Aktion kann mit mehreren Warnungsregeln verknüpft werden. Es gibt z. B. mehrere verschiedene Situationen, in denen ein IT-Manager in über eine Warnungsbedingung benachrichtigt werden möchte. Daher kann eine Aktion, die zum Senden einer E-Mail-Nachricht an den Manager führt, mit allen entsprechenden Warnungsregeln verknüpft werden.

Hinweis: Obwohl mit der Warnungsaktion "Externen ausführbaren Prozess starten" nur EXE-Dateien gestartet werden können, können Sie `cmd.exe` starten und mit Befehlszeilenargumenten nicht-EXE-Dateien wie BAT- oder VBS-Dateien aufrufen.

Informationen zum Erstellen von Warnungsaktionen finden Sie in der Onlinehilfe unter dem Stichwort "Warnungsaktionen".

Verwalten von Warnungsunterdrückungen

Auf der Seite "Warnungsunterdrückungen" (**Unternehmenskonfiguration > Warnungen > Unterdrückungen**) werden die Warnungen angezeigt, die unterdrückt wurden. Als Administrator können Sie alle Warnungsunterdrückungen bearbeiten und löschen.

Über die Warnungsliste auf der Registerkarte "Überwachen" kann jeder Benutzer Warnungsunterdrückungen erstellen. Diese Unterdrückungen hindern die EdgeSight Server Console am Anzeigen einer bestimmten Art von Warnungen, wobei als Entscheidungskriterium die Quelle, das Gerät, der Benutzer oder eine Kombination aus diesen Kriterien zugrunde gelegt wird. Beachten Sie, dass sich Unterdrückungen immer nur bei dem Benutzer auswirken, der sie erstellt hat. Andere Benutzer sehen die Warnungen auch weiterhin. Weitere Informationen zu Warnungsunterdrückungen finden Sie in der Onlinehilfe unter den Themen "Aktuelle Warnungsliste" und "Warnungsunterdrückungen".

Verwalten von Anwendungskategorien und Anbietern

EdgeSight enthält umfangreiche Anwendungskategorie- und Anbieterlisten, um Berichte nach Art der Anwendung oder nach Softwarehersteller erstellen zu können. In vielen Fällen fällt das Programm in eine vorhandene Kategorie und entspricht einem vorhandenen Anbieter. Wenn nötig, können Sie aber auch eine neue Kategorie oder einen neuen Anbieter für den neuen Prozess erstellen. Ausführliche Anweisungen zum Erstellen und Bearbeiten von Kategorien und Anbietern finden Sie in der Online-Hilfe in den Themen "Kategorien bearbeiten" und "Lieferanten bearbeiten".

Verwalten von Berichten

EdgeSight bietet eine breite Palette an Standardberichten. Diese Berichte sind verfügbar, nachdem EdgeSight Server installiert wurde und die Verbindung zu Reporting Services konfiguriert wurde.

Verwalten von Berichtsabonnements

Ein Abonnement ist eine dauerhafte Anforderung, einen Bericht in einem ausgewählten Format zu bestimmten Zeiten zu verteilen. Die Berichtsverteilung (Abonnementtyp) erfolgt per E-Mail oder durch Übertragen einer Datei auf eine Dateifreigabe. Abonnements können öffentlich oder privat sein. Öffentliche Abonnements werden auf der Registerkarte "Abonnements" des Berichtsdetailbereichs angezeigt. Private Abonnements werden nur dem Abonnementersteller oder einem Administrator angezeigt. Abonnements sind eine sinnvolle Methode der gezielten Verteilung von Daten an Personen in einer Organisation, ohne dass diesen dazu Zugriff auf die EdgeSight Server Console gewährt werden muss. Welche öffentlichen Abonnements vorhanden sind, können Sie unter **Eigene Einstellungen > Abonnements** anzeigen.

Sie können ein Abonnement erstellen, während Sie sich über den Link **Abonnieren** in der Filterleiste den Bericht ansehen. Sie können Abonnements aber auch von jeder Berichtsliste aus erstellen, indem Sie auf der Registerkarte "Abonnements" die Berichtseigenschaften anzeigen und dann auf die Schaltfläche **Neues Abonnement** klicken. Ausführliche Anweisungen zum Erstellen von Abonnements finden Sie in der Onlinehilfe im Thema "Arbeiten mit Berichten".

Als Administrator erhalten Sie standardmäßig die Berechtigungen, die zum Verwalten von öffentlichen und privaten Abonnements erforderlich sind. (Eine Beschreibung der Berechtigungen und ihrer Beziehung zu Rollen finden Sie unter "Erstellen von Benutzern und Zuweisen von Rollen" auf Seite 33.) Aufgrund dieser Berechtigungen sind Sie in der Lage, die Verteilung von Daten innerhalb Ihrer Organisation zu steuern und die Auswirkung auf den Berichtserver zu verwalten.

Hochladen von Berichten

Wenn Sie eine RDL-Datei für einen angepassten Bericht an den Berichtserver übertragen möchten, gehen Sie zur Seite "Angepasste Berichte" (**Eigene Einstellungen > Angepasste Berichte**) und klicken Sie dort auf **Bericht hochladen**.

Verwenden Sie beim Hochladen eines neuen Berichts immer einen eindeutigen Namen. Außerdem empfiehlt es sich, für angepasste Berichte Benennungsrichtlinien zu definieren und zu veröffentlichen. Über die Optionsfelder **Öffentlich** und **Privat** können Sie festlegen, ob der Bericht in Ihrem Unternehmen frei verfügbar sein soll. Öffentliche Berichte werden allen Benutzern angezeigt, sofern das Anzeigen des jeweiligen Berichts nicht durch die ausgewählten Berechtigungen eingeschränkt wird. Private Berichte werden nur dem Benutzer angezeigt, der den Bericht hochlädt. Das Ändern des Attributs "Öffentlich" in "Privat" und umgekehrt ist nach dem Hochladen des Berichts nicht mehr möglich. Wenn Sie dieses Attribut ändern möchten, müssen Sie den Bericht löschen und ihn dann erneut hochladen.

Wenn Sie weitere Änderungen am Bericht vornehmen, können Sie die RDL (Report Definition Language)-Datei über den Link **Aktualisieren** auf der Seite "Eigenschaften" hochladen. Weitere Informationen dazu finden Sie in der Onlinehilfe in den Themen "Angepasste Berichte" und "Upload von angepasstem Bericht".

Verwalten von IP-Bereichen

Durch Festlegen von IP-Bereichen können Sie das Unternehmensnetzwerk definieren, das zum Filtern des Netzwerks nach Unternehmens- oder externen Netzwerkhosts verwendet werden soll. Auf dieser Seite definierte Bereiche von IP-Adressen werden als Unternehmensnetzwerkstandorte dargestellt. Diese Option ist nur erforderlich, wenn die von Ihnen verwendete IP-Adresse im privaten, nicht-externen IP-Adressbereich nicht definiert ist. Anweisungen zum Festlegen von IP-Bereichen finden Sie in der Onlinehilfe im Abschnitt "IP-Bereiche".

Verwalten von Echtzeit-Dashboard-Konfigurationen

In EdgeSight steht Ihnen ein Dashboard zur Verfügung, über das Sie auf der Grundlage einer gespeicherten Konfiguration Echtzeitinformationen für bestimmte Geräte und Indikatoren anzeigen können. Das Dashboard wird auf der Registerkarte "Überwachen" angezeigt. Zum Erstellen und Bearbeiten benannter Konfigurationen für das Dashboard steht Ihnen die Seite "Echtzeitkonfigurationen" zur Verfügung. Die Konfigurationen enthalten einen eindeutigen Namen, Festlegungen zu Timeouts für Abfragen und Verbindungen, ein Aktualisierungsintervall sowie Angaben dazu, welche Leistungsindikatoren für die ausgewählten Geräte angezeigt werden. Pro Konfiguration können Sie maximal 20 Geräte und 8 Leistungsindikatoren auswählen. Ausführliche Anweisungen zum Erstellen und Bearbeiten der Konfigurationen finden Sie in der Onlinehilfe im Abschnitt "Echtzeitkonfigurationen". Beachten Sie, dass auf den Geräten ein EdgeSight-Agent der Version 4.2 oder höher ausgeführt werden muss, damit sie im Dashboard angezeigt werden.

Nach dem Erstellen einer Konfiguration wird diese der Dropdownliste auf der Seite "Dashboard" hinzugefügt. Von dort aus kann der Benutzer dann die gewünschte Konfiguration für die Anzeige im Dashboard auswählen. Die im Dashboard angezeigten Daten basieren auf direkten Abfragen verwalteter Geräte. Die Dashboard-Daten werden nicht auf dem Server gespeichert.

Festlegen von Agenteigenschaften

Der EdgeSight-Agent speichert Konfigurationsdaten an zwei Speicherorten. Konfigurationseinstellungen, die computerspezifisch und für die erfolgreiche Kommunikation mit dem EdgeSight Server erforderlich sind, werden in der Windows-Registrierung auf dem verwalteten Gerät gespeichert. So werden z. B. in der Registrierung der Name des Unternehmens, zu dem der Agent gehört, der Name des Servers, der kontaktiert werden muss, sowie alle Proxyinformationen gespeichert, die für die Kommunikation benötigt werden. Alle anderen Konfigurationseinstellungen werden in der EdgeSight-Agentdatenbank gespeichert. Wenn der Agent auf einem virtuellen Desktop in einer gepoolten Umgebung ausgeführt wird, befindet sich die Agentdatenbank auf einem Remoteserver.

Die Einstellungen, die in der Windows-Registrierung gespeichert werden, werden in der Regel nur einmal festgelegt und während der Agentinstallation bereitgestellt. Alle anderen Konfigurationseinstellungen werden vom zugeordneten EdgeSight-Server bereitgestellt und sämtliche Änderungen an der Konfiguration werden über die Seite "Agenteigenschaften" vorgenommen. Standardmäßig erhält ein Agent seine Erstkonfiguration, kurz nachdem der Agent zum ersten Mal ausgeführt wird. Anschließend prüft er die Konfiguration auf Änderungen. Der Standardzeitplan für diese Konfigurationsprüfungen sieht vor, dass die Prüfung jeden Tag um 6:30 Uhr (lokale Zeit des Agents) für Endpunktgeräte und einmal pro Stunde für XenApp-Server erfolgt. Agents, die auf virtuellen Desktops in einer gepoolten Umgebung ausgeführt werden, prüfen die Konfiguration basierend auf der tatsächlichen Nutzung.

Das Ändern von Agenteigenschaften sollte mit Bedacht erfolgen. Diese Parameter steuern die Funktionsweise des Agents und können dazu führen, dass ein Datenverlust oder eine gestiegene CPU-Nutzung durch den Agent auftritt. In den meisten Fällen müssen die Agenteigenschaften nicht angepasst werden. Verwenden Sie zunächst die Standardkonfiguration und passen Sie diese nach und nach an den Benutzerbedarf und die Systemleistung an.

Agentkonfigurationen werden auf der Seite Agenteigenschaften angezeigt (**Unternehmenskonfiguration > Agents > Eigenschaften**). Beim Erstellen eines neuen Satzes Agenteigenschaften müssen Sie eine Standardkonfiguration ("Endpunktstandard", "XenApp-Standard" oder "Standard für virtuellen Desktop") als Vorlage auswählen. Geben Sie dann einen eindeutigen Namen und eine Beschreibung für die Konfiguration ein und bearbeiten Sie die Parameter wie gewünscht.

Hinweis: Wenn Sie ein Upgrade von einer EdgeSight Server-Version vor 5.0 SP2 durchgeführt haben, wird die Standardkonfiguration für virtuelle Desktops erst nicht in der Liste der Agenteigenschaftkonfigurationen angezeigt. Um Agenteigenschaftseinstellungen für virtuelle Desktops zu erstellen, klicken Sie auf **Konfiguration neuer Eigenschaften** und aktivieren Sie dann das Optionsfeld **Standardeigenschaften für Agents für virtuelle Desktops**. Konfigurieren Sie die Eigenschaften wie in der Onlinehilfe im Abschnitt "Assistent für Agenteigenschaften" beschrieben.

Nachdem Sie einen neuen Satz Agenteigenschaften erstellt haben, muss dieser explizit einer Abteilung zugeordnet werden. Erst dann wird sie Agents im Rahmen einer Konfigurationsprüfung bereitgestellt. (Informationen zum Verknüpfen eines Satzes von Agenteigenschaften mit Abteilungen finden Sie unter "Verwalten von Abteilungen" auf Seite 28.)

Informationen zu den einzelnen Parametern von Agenteigenschaften finden Sie in der Onlinehilfe im Abschnitt "Assistent für Agenteigenschaften".

Minimaldatensammlungsmodus

Zur Unterstützung stark beanspruchter XenApp-Server besitzt der EdgeSight-Agent einen Minimaldatensammlungsmodus, der, sofern aktiviert, die auf dem Agent erfassten Daten einschränkt und damit den Gesamteinfluss des Agents auf den XenApp-Server mindert.

Wenn ein XenApp-Server durchgehend eine starke Auslastung aufweist oder unter Last sehr langsam wird, sollte diese Funktion verwendet werden. Notieren Sie sich anhand der EdgeSight-Berichte, in wie vielen Sitzungen und Prozessen es zu einer signifikanten Verlangsamung kommt. Diese Werte werden verwendet, um festzulegen, wann der Minimaldatensammlungsmodus auf dem Agent eingeleitet wird.

Hinweis: Der Minimaldatensammlungsmodus ist als vorübergehende Maßnahme anzusehen, mit der sichergestellt werden kann, dass kritische Daten erfasst werden. Zusätzlich können auch langfristige Maßnahmen ergriffen werden, um die Last auf den betroffenen XenApp-Servern zu verringern oder neu zu verteilen.

Der Minimaldatensammlungsmodus ist standardmäßig deaktiviert. Um ihn zu aktivieren, bearbeiten Sie die Agenteigenschaften und zeigen die erweiterten Einstellungen an. Legen Sie für Datenerfassung verwalten den Wert Wahr fest und geben Sie in die Felder Prozessanzahl-Schwellenwert und Sitzungszahl-Schwellenwert Werte ein, die Sie gesammelt haben. Weisen Sie anschließend diesen Satz Agenteigenschaften dem XenApp-Server zu, auf dem das Problem auftritt.

Wenn der Minimaldatensammlungsmodus aktiviert ist, wird die Prozess- und Sitzungsanzahl vom Agent unter Berücksichtigung der konfigurierten Schwellenwerte regelmäßig überwacht. Wenn ein Schwellenwert den für ihn angegebenen Wert überschreitet, wird vom Agent der Minimaldatensammlungsmodus aktiviert. An diesem Punkt wird eine Betriebswarnung an den Server gesendet, die angibt, dass vom Citrix System Monitoring Agent der Minimaldatensammlungsmodus aktiviert wurde. Wenn die Werte für Prozess- und Sitzungsanzahl 5 Minuten lang unter die Schwellenwerteinstellungen fallen, wird der Minimaldatensammlungsmodus durch den Agent beendet und die normale Datensammlung fortgesetzt. Ein Eintrag wird an den Server gesendet, um anzugeben, dass der Minimaldatensammlungsmodus vom Agent beendet wurde.

Die Minimaldatensammlung unterscheidet sich wie folgt von der normalen Datensammlung:

- Es werden keine Moduldaten gesammelt oder gespeichert.
- Es werden keine Netzwerkdaten gesammelt oder gespeichert.
- Es werden keine Light-Trace-Ereignisse gespeichert.
- Es werden keine Image- oder Prinzipalereignisse gespeichert (derzeit nicht sichtbar).
- Es werden keine in Fehlerberichten verwendeten Aufgabendetails gespeichert.
- Die Erkennung nicht reagierender Anwendungen ist deaktiviert.
- Image- und Sitzungsleistungsdaten werden in einem 2-Minuten-Intervall gespeichert.
- Die Sammlung benutzerdefinierter Leistungsindikatoren ist deaktiviert.
- Leistungs-, Netzwerk- und Ereignisverfolgungswarnungen sind deaktiviert.

EdgeSight für XenApp enthält darüber hinaus die folgenden Konfigurationsänderungen:

- Detailgenaue System-, Image- und Sitzungsleistungsdaten werden in 15-Sekunden-Intervallen gespeichert.
- Wenn der Planer mehr als 5 gleichzeitig aktive Sitzungen erkennt, wird nicht die Inaktivität für die Entscheidung herangezogen, wann geplante Elemente wie eine Konsolidierung ausgeführt werden können. Stattdessen wird angenommen, dass es sich hierbei um ein Serversystem handelt und es deshalb nie geeignete Inaktivitätsphasen zum Ausführen von Zeitplänen gibt.
- Es können einzelne Worker auf dem Server konfiguriert werden, um bei der Ermittlung der optimalen Ausführungszeit die Inaktivität auf ähnliche Weise zu ignorieren.

Konfigurieren, Terminieren und Ausführen von Workern

Worker sind Aufgaben, die von EdgeSight-Agents ausgeführt werden. Bei der EdgeSight Server-Installation werden Standardworkerkonfigurationen und Standardzeitpläne erstellt. Standardkonfigurationen und -zeitpläne können weder bearbeitet noch gelöscht werden, Sie können diese aber kopieren, um sie als Vorlagen zu verwenden, und dann die Parameter wie gewünscht bearbeiten.

Die Ausführung von Workern ist zwar auf bestimmte Zeiten terminiert, wann sie aber tatsächlich ausgeführt werden, hängt davon ab, wann ein Benutzer das System aktiv verwendet. Wenn möglich, werden Worker ausgeführt, wenn das System inaktiv ist. Weitere Informationen zum Festlegen von Zeitplänen für Worker finden Sie unter "Konfigurieren von Workern" auf Seite 54.

Genau wie bei den Agentkonfigurationen sollten auch Workerkonfigurationsparameter nur mit Vorsicht geändert werden. Diese Parameter steuern, wann und wie oft Worker ausgeführt werden. Änderungen können zur Folge haben, dass die Benutzer eine höhere CPU-Nutzung durch den Agent feststellen. In der Mehrzahl der Fälle müssen Sie keine angepassten Workerkonfigurationen erstellen. Verwenden Sie zunächst die Standardkonfiguration und passen Sie diese nach und nach an den Benutzerbedarf und die Systemleistung an.

Nach dem Erstellen einer angepassten Workerkonfiguration muss diese explizit einer Abteilung zugeordnet werden. Erst dann wird sie Agents im Rahmen einer Konfigurationsprüfung bereitgestellt. (Informationen zum Verknüpfen von Workerkonfigurationen mit Abteilungen finden Sie unter "Verwalten von Abteilungen" auf Seite 28.)

Sie können folgende EdgeSight-Worker konfigurieren:

- **Anlagenliste:** Stellt eine Anlagenliste für die verwalteten Geräte zusammen. Dieser Worker kann deaktiviert werden.
- **Konfigurationsüberprüfung:** Prüft die Konfiguration auf Änderungen, die vom Server auf verwaltete Geräte heruntergeladen werden müssen.
- **Datenbankwartung:** Führt Datenbankwartungsaufgaben in der Agentdatenbank aus.
- **Berechnung von Speicherplatz auf Laufwerk:** Berechnet den auf verwalteten Geräten genutzten Festplattenspeicherplatz. Dieser Worker kann deaktiviert werden.
- **Bereinigung des Ausfallberichts:** Wartet und bereinigt Dateien, die für Fehler- und Snapshot-Berichte erstellt wurden.
- **Leistungsupload:** Lädt Agentdaten auf den EdgeSight-Server hoch.

Konfigurieren von Workern

Eine Workerkonfiguration enthält die folgenden Komponenten:

- Konfigurationsname und -beschreibung: Der Name und die Beschreibung sollten möglichst aussagekräftig sein, um Administratoren die Auswahl der richtigen Konfiguration zu erleichtern.
- Satz aktivierter Worker: Nur die Worker "Anlagenliste" und "Berechnung des Festplattenspeichers" können deaktiviert werden. Für einen ordnungsgemäßen Systembetrieb müssen alle anderen Worker ausgeführt werden.
- Satz Ausführungsbedingungen: Zusätzlich zum Workerzeitplan wird das Verhalten des Workers durch einen Satz Ausführungsbedingungen gesteuert.
- Mindestens ein Zeitplan: Für jeden aktivierten Worker muss mindestens ein Zeitplan konfiguriert sein, der zusammen mit den Ausführungsbedingungen bestimmt, wann der Worker ausgeführt wird.

Die Ausführungsbedingungen für Worker lauten folgendermaßen. Es sind nicht alle Ausführungsbedingungen für alle Worker festgelegt.

- "Tage, bevor der Worker automatisch ausgeführt wird": Diese Einstellung gibt an, dass der Worker nach der angegebenen Anzahl von Tagen ausgeführt wird, und dies auch dann, wenn andere Bedingungen (z. B. Inaktivität eines Benutzers) nicht erfüllt sind. Wenn der Worker aufgrund von Kommunikationsproblemen nicht ausgeführt werden kann, wird er ausgeführt, sobald die Kommunikation wiederhergestellt ist.
- "Zufälliger Start in einem Fenster von": Um die System- und Netzwerkleistung aufrechtzuerhalten, kann für die Ausführung der Worker festgelegt werden, dass sie innerhalb eines Zeitfensters zufllig starten. Dadurch werden z. B. Situationen vermieden, in denen eine große Anzahl von Agents versucht, zum gleichen Zeitpunkt Leistungsdaten hochladen.
- System als inaktiv betrachten, wenn alle Benutzer inaktiv für: Diese Einstellung sorgt dafür, dass Worker dann ausgeführt werden, wenn Benutzer die Systeme nicht aktiv verwenden. (Der Worker-Zeitplan hat eine ähnliche Option: **Mit dem Starten des Workers warten, bis alle Benutzer inaktiv sind**.)

Eine Ausführungsbedingung muss einen Wert ungleich null enthalten, um aktiviert zu werden. Durch eine Null als Wert für eine Ausführungsbedingung wird diese Bedingung automatisch deaktiviert. Weitere Informationen zum Konfigurieren von Workern finden Sie in der Onlinehilfe im Abschnitt "Assistent zum Konfigurieren von Workern".

Überwachen von Workern

Einige Worker zeichnen Informationen in Protokolldateien auf. Der Datei `SYS_EVENT_TXT.txt` können Sie entnehmen, welche Worker wann ausgeführt wurden. Sie finden diese Datei standardmäßig in Ihrem Installationspfad:

`%ALLUSERSPROFILE%\Citrix\System Monitoring\Data` für Microsoft Vista- und Windows 2008-Systeme

`%ALLUSERSPROFILE%\Anwendungsdaten\Citrix\System Monitoring\Data` für alle anderen Systeme

Für Agents, die auf virtuellen Desktops in Pools ausgeführt werden, werden die Protokolldateien auf eine Dateifreigabe für Agentdaten kopiert, die während der Agentinstallation angegeben wurde.

In dieser Datei werden auch alle Fehler protokolliert, die beim Versuch aufgetreten sind, einen bestimmten Worker auszuführen. Dadurch wird die Diagnose der Probleme vereinfacht. Beachten Sie, dass Worker, die produktintern sind und zur Produktwartung dienen, keine Protokolldatei erstellen. In den folgenden Listen sind die Worker nach der Art der Aufgabe zusammengefasst, die sie ausführen:

Worker, die mit dem Server interagieren:

- Worker 101: "Leistungsupload" – Lädt Agentdaten auf den EdgeSight-Server hoch.
- Worker 104: Init-Worker - Wird auf der ursprünglichen Datenbankerstellung ausgeführt, stellt eine Verbindung zum Server her und lädt erste Agenteigenschaften herunter.
- Worker 105: "Konfigurationsüberprüfung" – Prüft die Konfiguration auf Änderungen.
- Worker 109: "Routenverfolgungs-Worker" – Führt eine Netzwerkverfolgung aus.
- Worker 150: "Bullet-Worker" – Lädt Warnungsinformationen auf den EdgeSight-Server hoch.

Worker, die Daten erfassen:

- Worker 102: "Berechnung des Festplattenspeichers" – Berechnet, wie viel freier Speicherplatz auf dem Gerät vorhanden ist.
- Worker 103: "Anlagenliste" – Stellt eine Anlagenliste der verwalteten Geräte zusammen.

Worker, die den Agent warten:

- Worker 1: "Feinabstimmung der Datenbank" – Interne Wartung, es erfolgt keine Protokollierung.
- Worker 2: "Datenbankwartung" – Interne Wartung, es erfolgt keine Protokollierung.
- Worker 106: "AD-Worker" – Führt ein Active Directory-Skript aus.
- Worker 107: "Bereinigung des Ausfallberichts" – Wartet und bereinigt Dateien, die für Ausfall- und Snapshot-Berichte erstellt wurden.
- Worker 108: "Ausfallberichtvorbereitung" – Erstellt Ausfallberichte und lädt diese auf den Server hoch.
- Worker 110: "Bereinigung des RISH-Protokolls" – Wartet und bereinigt Protokolle, die aus RISH erstellt wurden.
- Worker 126: "Datenbankgrößenanpassung" – Nimmt eine Feinabstimmung der Datenbankgröße vor.

Sie finden in diesem Verzeichnis eventuell auch noch andere Protokolle, die hier nicht beschrieben wurden. Ursache dafür ist, dass einige Warnungen als Skripte ausgeführt und deren Aktivitäten protokolliert werden.

Die Workerprotokolldateien enthalten Informationen, die bei der Behebung von Fehlern hilfreich sein können, die im Zusammenhang mit den verschiedenen, vom Agent ausgeführten Arbeitsfunktionen auftreten können. Wenn Sie überprüfen möchten, ob es bei einem Worker zu einem Problem gekommen ist, sollten Sie zuerst in der Datei `SYS_EVENT_TXT.txt` nachsehen. Anhand der Informationen in dieser Datei können Sie dann im Protokoll des konkreten Workers nach detaillierteren Informationen suchen.

Angenommen, die Datei `SYS_EVENT_TXT.txt` enthält einen Hinweis auf die folgende Fehlermeldung:

```
Running worker 101 - 'Performance Upload' with trigger 1071
```

Sie müssten dann im Protokollordner für die Textdatei nachsehen, die mit `Worker101_Trigger1071` beginnt.

Die nützlichsten Protokolle sind normalerweise die, die für die Upload- und Konfigurationsworker erstellt werden, da mit ihrer Hilfe Konnektivitätsprobleme zwischen Agent und Server gelöst werden können. Aus diesem Grund sind die Protokolle für die Worker 101, 104 und 105 in der Regel am ehesten für die Behebung von Problemen dieser Art geeignet. So können Sie z. B. sichergehen, dass die Kommunikation zwischen dem Agent und dem Server nicht geklappt hat, indem Sie die Datei `SYS_EVENT_TXT` prüfen, nach Worker 104 suchen, der mit Trigger 24 ausgeführt wird, und dann feststellen, dass ein anderer Status als 0x0 angezeigt wird.

Fehlerbehebung anhand von Agentprotokolldateien

Auf den Geräten, auf denen der Agent ausgeführt wird, sind folgende Protokolldateien vorhanden, anhand derer Probleme mit der Kommunikation zwischen Agent und Server besser diagnostiziert werden können. Beachten Sie, dass für Agents, die auf virtuellen Desktops ausgeführt werden, die Protokolldateien auf eine Dateifreigabe für Agentdaten kopiert werden, die während der Agentinstallation angegeben wurde.

- System- und Anwendungsereignisprotokolle (in der Ereignisanzeige)
- EdgeSight-Hauptprotokolldatei, standardmäßig gespeichert unter:

```
%ALLUSERSPROFILE%\Anwendungsdaten\Citrix\System Monitoring\Data\#
SYS_EVENT_TXT.txt
```

- Einzelne Worker-Protokolldateien (siehe "Überwachen von Workern" auf Seite 55), standardmäßig gespeichert unter:

```
%ALLUSERSPROFILE%\Anwendungsdaten\Citrix\System Monitoring\Data\#
EdgeSight\log
```

Wenn Sie auf ein Problem stoßen, das Sie nicht selbst lösen können, und Sie den technischen Support kontaktieren müssen, halten Sie bitte die Versionsnummern des Agents und der Serversoftware bereit. So können Sie die Angaben zur jeweiligen Produktversion ermitteln:

- Agent: Öffnen Sie die Datei SYS_EVENT_TXT. Beim Starten fügt der Agent eine Zeile in etwa folgender Form ein:

```
----- Starting Agent on Computername version 5.0.74.0 -----
```

- Server: Öffnen Sie die EdgeSight Console und wählen Sie **Serverstatus > Info**. Neben Reflectent.EdgeSight.Loader.dll wird die richtige Version angezeigt.

Verwalten von Servereinstellungen

In diesem Kapitel wird beschrieben, wie Sie globale Einstellungen auf einem Citrix EdgeSight-Server verwalten können. Die Konsolenseiten, die in diesem Kapitel beschrieben wird, befinden sich auf der Registerkarte **Konfiguration** in den Bereichen **Serverkonfiguration** und **Serverstatus**. Informationen zum Verwalten unternehmensspezifischer Einstellungen finden Sie in Kapitel 2, "Verwalten von Unternehmenseinstellungen" . Dieses Kapitel enthält eine Beschreibung der folgenden Aufgaben:

- Überwachen des Serverstatus
- Konfigurieren von Servereinstellungen
- Erstellen von Unternehmen
- Konfigurieren von Datenuploads
- Verwalten von Lizenzen
- Verwalten von Authentifizierungsprovidern
- Konfigurieren der Verbindung zu Reporting Services
- Verwalten von Reporting Services-Zeitplänen
- Verwalten der Datenbank
- Umgang mit nicht verwalteten Geräten
- Anzeigen des Status des Agentdatenbankbrokers
- Anzeigen von und Reagieren auf Servernachrichten
- Verwalten von Serverskripts

Überwachen des Serverstatus

Auf der Seite "Status" (**Serverkonfiguration > Status**) können Sie sich einen Überblick über die Serveroperationen in den einzelnen Unternehmen verschaffen. Die Tabelle "Unternehmen" enthält nach Unternehmen geordnete Angaben dazu, wie viele Gerte an diesem Tag Daten auf den Server hochgeladen und wie viele Geräte keine Daten auf den Server hochgeladen haben. Außerdem können Sie dieser Tabelle entnehmen, wie viele neue Geräte, auf denen EdgeSight Agent ausgeführt wird, sich an diesem Tag und in der vorhergehenden Woche beim Server registriert haben. Beim Status für Nachrichten, nicht verwaltete Geräte, Warnungen und Absturzberichte handelt es sich einfach um die Anzahl der jeweiligen Aktivitäten für den aktuellen Tag.

Statustyp	Vorgehensweise zur Anzeige detaillierter Informationen
Unternehmen:	Wählen Sie **Unternehmenskonfiguration > Geräteverwaltung > Geräte**, um zu sehen, wann bestimmte Geräte Daten auf den Server hochgeladen haben, und um Informationen zu neuen Geräten aufzurufen.
Server Script Host-Status	Klicken Sie auf **Server Script Host**, um die Seite "Server Script Host" zu öffnen. Wählen Sie **Serverkonfiguration > Einstellungen** und klicken Sie auf die entsprechende Registerkarte, um Einstellungen für "Datenupload" und "Absturzverarbeitung" anzuzeigen und zu verwalten.
Nachrichtenstatus	Klicken Sie auf **Nachrichtenstatus**, um die neuesten Nachrichten anzuzeigen.
Nicht verwaltete Geräte	Klicken Sie auf **Nicht verwaltete Geräte**, um Informationen zu nicht verwalteten Geräten anzuzeigen. Ein nicht verwaltetes Gerät ist ein System mit installiertem EdgeSight-Agent, das keinem Unternehmen und keiner Abteilung zugeordnet ist.
Warnungen	Öffnen Sie die Registerkarte **Überwachen** und wählen Sie entweder **Warnungskonsole** oder **Warnungsliste**, um Informationen zu den jüngsten Warnungsbenachrichtigungen anzuzeigen. Weitere Informationen zu Warnungen finden Sie unter "Erstellen von Regeln und Aktionen für Warnungen" auf Seite 35.
Absturzberichte	Öffnen Sie die Registerkarte **Überwachen**, wählen Sie **Warnungsliste** und filtern Sie nach Warnungen für prozessorinterne Prozessfehler oder Prozess-Snapshots. Weitere Informationen zum Zugreifen und Verwenden von Absturzberichten finden Sie in der *Citrix EdgeSight-Benutzerdokumentation*.

Konfigurieren von Servereinstellungen

Auf der Seite "Betriebskonfiguration" (**Serverkonfiguration > Einstellungen**) können Sie steuern, wie EdgeSight Server die folgenden Funktionen handhabt:

- Agentunterstützung und Lizenzserver
- Protokollierung für Agentdatenbankbroker
- Benachrichtigungen
- Timeouts
- Datenupload
- Anwendungsabsturzverarbeitung
- SSL-Unterstützung
- SNMP-Port

Die Werte und Einstellungen auf dieser Seite brauchen im Normalfall nicht geändert zu werden. Wir empfehlen, die Standardeinstellungen zu verwenden und die Serverleistung unter Produktionsbedingungen zu beobachten, bevor Anpassungen an den Servereinstellungen in Erwägung gezogen werden. Eine Definition der einzelnen Einstellungen finden Sie in der Onlinehilfe im Abschnitt "Serverkonfigurationseinstellungen".

Agentunterstützung und Lizenzserver

Je nach den in Ihrer Umgebung installierten Citrix EdgeSight-Produkten können Sie festlegen, ob Berichte mit XenApp-Server- oder Endpunktdaten angezeigt werden sollen. Außerdem können Sie durch Wählen der Option "Standard" oder "Erweitert" festlegen, in welchem Umfang Unterstützung für EdgeSight für XenApp Agents angeboten wird.

- *Standard*-Agents bieten die Ressourcenverwaltungsfunktionen, die Teil von XenApp Enterprise Edition sind. Hierfür ist nur erforderlich, dass Sie eine XenApp Enterprise-Lizenz auf Ihrem Citrix Lizenzserver haben. Der Agent zeichnet Informationen zur Client- und Serverleistung und zur Anwendungsnutzung auf.

- *Erweiterte* Agents bieten den vollen Funktionsumfang von EdgeSight für XenApp. Hierfür benötigen Sie entweder eine XenApp Platinum Edition-Lizenz oder eine EdgeSight für XenApp-Lizenz auf Ihrem Citrix Lizenzserver. Der Agent zeichnet Informationen zu Benutzersitzungen, zur Client- und Serverleistung, zur Anwendungsverwendung und zu den Netzwerkverbindungen auf.

Diese Einstellung wirkt sich nur darauf aus, ob Berichte und Verwaltungsseiten in der Konsole angezeigt werden. Daten werden auch dann weiterhin erfasst, hochgeladen und gespeichert, wenn die Anzeigeunterstützung deaktiviert ist. Beachten Sie, dass dies im Unterschied zu den Einstellungen für die Warnungsunterdrückung eine Einstellung ist, die sich serverweit auswirkt und von der abhängt, was alle Benutzer beim Verwenden der Konsole sehen. Weitere Informationen dazu, welche Tools und Berichte für die Agenttypen angezeigt werden, finden Sie unter "Verwenden von EdgeSight in gemischten Umgebungen" auf Seite 83.

Zum Aktivieren oder Deaktivieren der Unterstützung wählen Sie die entsprechende Option aus den Unterstützung-Dropdownlisten aus. Wenn Sie sich für eine Option entscheiden, durch die verfügbare Daten von der Anzeige ausgeschlossen werden, z. B. wenn Sie XenApp-Agentunterstützung für einen Server deaktivieren, der Daten von EdgeSight für XenApp Agents erhält, wird ein Bestätigungsfeld angezeigt.

Wenn die Option "Unterstützung von EdgeSight für Endpunkte" aktiviert ist, können Sie auch den Namen und den Port des Citrix Lizenzservers bearbeiten, der die Lizenzen für Endpunktsysteme liefert.

Protokollierung für Agentdatenbankbroker

Auf der Registerkarte "Agentdatenbankbroker" können Sie die Anzeige von detaillierten Brokerprotokollmeldungen aktivieren. Diese Option ist standardmäßig deaktiviert. Wenn diese Option aktiviert ist, werden auf der Seite "Brokerverlauf" zusätzliche Statusmeldungen angezeigt. (Weitere Informationen dazu finden Sie unter "Anzeigen des Brokerverlaufs" auf Seite 80.) Auf dem Agentdatenbankbroker findet immer detaillierte Protokollierung statt; mit dieser Funktion wird lediglich die Anzeige von Daten auf der Seite "Brokerverlauf" gesteuert. Die Funktion ist nützlich, um detaillierte Informationen für die Fehlerbehebung von Problemen beim Agentdatenbankbroker zu erhalten.

Benachrichtigungen

Der Name und die E-Mail-Adressen des SMTP-Servers müssen während der Serverinstallation angegeben werden, können aber bei Bedarf geändert werden.

Wichtig: Für den Serverbetrieb ist es absolut wichtig, dass ein gültiger SMTP-Servername verwendet wird. EdgeSight Server verwendet den SMTP-Server für viele Funktionen, darunter für die Verteilung von Warnungsbenachrichtigungen, Serverfehlerbedingungen und neuen Benutzerkennwörtern.

Die folgende Tabelle enthält eine Zusammenstellung der Benachrichtigungsoptionen. Die E-Mail-Optionen ermöglichen es dem Server, im Falle eines Agent- oder Serverfehlers E-Mails an die E-Mail-Adresse des EdgeSight-Administrators zu senden.

Option	Beschreibung
Neue Agents	Diese Option eignet sich hervorragend, wenn ein Administrator per E-Mail benachrichtigt werden soll, dass neue Geräte Daten auf den Server hochladen. Die Clientregistrierung wird durch die unter "Verwalten von Unternehmenseinstellungen" auf Seite 26 beschriebenen unternehmensspezifischen Einstellungen gesteuert.
Agent-Fehler	Diese Option können Sie bei der ersten Verwendung von Citrix EdgeSight Server aktivieren, um Probleme mit Agenteigenschaften aufzuspüren und zu beheben. Wenn diese Probleme behoben wurden, ist diese Option ggf. nicht mehr erforderlich. In der Regel sind Agents in der Lage, sich nach Fehlern automatisch wiederherzustellen.
Serverfehler	Diese Option können Sie bei der ersten Verwendung von Citrix EdgeSight Server aktivieren, um Konfigurationsprobleme aufzuspüren und zu beheben. Wenn diese Probleme behoben wurden, ist diese Option ggf. nicht mehr erforderlich.
Kommunikationsfehler	Diese Option eignet sich hervorragend, um einen Administrator zu benachrichtigen, wenn es Gerätekommunikationsprobleme gibt.
Fehler beim Lesen der HTTP-Nutzdaten (nicht empfohlen)	Diese Option sollte im normalen Gebrauch nicht verwendet werden, da bei Bedarf erneut versucht wird, die Nutzdaten hochzuladen. Ggf. können Sie diese Option zum Debuggen bestimmter Probleme beim Hochladen von Nutzdaten aktivieren.
Nutzdaten anhängen	Diese Option sollte im normalen Gebrauch nicht verwendet werden, da bei Bedarf erneut versucht wird, die Nutzdaten hochzuladen. Wenn diese Probleme behoben wurden, ist diese Option ggf. nicht mehr erforderlich.

Timeouts

Timeouts werden für häufige Serveroperationen (wie z. B. das Abfragen von Datenbanken und das Laden der ASP-Seite, das Anfordern von Datenuploads und das Abfragen von Hintergrunddiensten) festgelegt, um zu verhindern, dass der Server beim Warten auf eine Antwort auf eine Abfrage blockiert wird. Wir empfehlen, die Standardwerte zu verwenden, es sei denn, ein bestimmtes Problem produziert ungewöhnlich viele Timeouts.

Beachten Sie, dass die Farmüberwachung und die Warnungskonsole (auf der Registerkarte "Überwachung") beim Abfragen von Warnungsdaten das ASP.NET Page and Query-Timeout verwenden. Wenn es bei der Verwendung dieser Seiten häufig zu Timeouts kommt, erhöhen Sie den Wert für ASP.NET Page and Query-Timeout nach Bedarf.

Datenupload

Der Upload von Daten bezieht sich auf die Erfassung von in der Warteschlange befindlichen Nutzdaten aus Datenbanken auf Computern, auf denen ein EdgeSight-Agent ausgeführt wird. Im Normalfall reichen die Standardwerte für einen ordnungsgemäßen Betrieb aus. Die Werte sollten nur dann angepasst werden, wenn Sie wiederholt wegen zu vieler Nutzdaten in der Warteschlange oder anderen Problemen beim Upload der Daten gewarnt werden. Hinweis: Die Mindesteinstellungen für CPU, Speicher und die "Aktive Zeit"-Timeouts haben die Aufgabe sicherzustellen, dass nur Daten von Computern mit einer bestimmten Mindestaktivität auf den Server hochgeladen werden. Auf diese Weise erhalten Sie einen exakten Überblick über die Verfügbarkeits- und Leistungsdaten im ganzen Unternehmen.

Anwendungsabsturzverarbeitung

Da die Anwendungsabsturzprotokolle recht groß werden können, besteht die Möglichkeit, die Aufbewahrung von Absturzprotokollen nach Anzahl, Festplattenspeicherplatz und Datum einzuschränken. Diese Grenzwerte helfen zu verhindern, dass die Absturzprotokolle zu viel Speicherplatz auf dem Server belegen. Sie können die Anwendungsabsturzverarbeitung auch deaktivieren. In diesem Fall werden keine Absturzprotokolldateien auf den Server hochgeladen.

Bei Überschreiten entweder der maximalen Anzahl von Absturzprotokollen oder des maximalen Speicherplatzes wird die Anwendungsabsturzverarbeitung automatisch deaktiviert, bis der Grenzwert erhöht wird. Es gibt keine Vorgänge zum Zurücksetzen, um vorhandene Nutzdaten zu entfernen.

SSL-Unterstützung

Die Funktion "SSL-Unterstützung" sorgt für sichere Anmeldungen. Auf dem Server, auf dem die EdgeSight-Website ausgeführt wird, muss ein gültiges SSL-Zertifikat vorhanden sein, das von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde. Wenn die SSL-Unterstützung aktiviert ist, muss die gesamte Kommunikation vom Agent zum Server über SSL erfolgen. Wenn ein Agent versucht, ohne SSL eine Verbindung mit einem SSL-aktivierten Server herzustellen, wird ein Fehler generiert. Alle Versuche, eine Verbindung zum Agent herzustellen (z. B. durch Remoteausführung eines Workers oder Anzeigen eines Echtzeitberichts), führen zur Ausgabe einer Fehlermeldung, der zufolge SSL erforderlich ist, diese Verbindung aber nicht über SSL aufgebaut wurde.

SNMP

Der SNMP-Trap-Port wird für ausgehende SNMP-Trap-Warnungen verwendet. Diese Porteinstellung wird für alle SNMP-Trap-Warnungen verwendet, die für alle Unternehmen definiert sind, die auf dem Server gehostet werden. Mit EdgeSight können Sie den Port festlegen. Dadurch vermeiden Sie Konflikte mit anderen Verwaltungstools, die möglicherweise den Standard-SNMP-Port für ausgehende Nachrichten verwenden. Weitere Informationen zum Erstellen von SNMP-Trap-Warnungen finden Sie unter "Erstellen von Regeln und Aktionen für Warnungen" auf Seite 35.

Erstellen von Unternehmen

Unternehmen sind die primäre Organisationseinheit auf einem EdgeSight-Server. Ein einzelner Server kann mehrere Unternehmen unterstützen. Ein erstes Unternehmen erstellen Sie, wenn Sie EdgeSight Server installieren. Nach dem Installieren und Konfigurieren können Sie bei Bedarf weitere Unternehmen erstellen. Wählen Sie dazu **Serverkonfiguration > Unternehmen**.

Zum Erstellen eines Unternehmens müssen Sie lediglich einen Namen und eine Zeitzone Standardsprache angeben. Unternehmensnamen müssen serverweit eindeutig sein. Wenn bei Ihnen mehrere EdgeSight-Server vorhanden sind und Sie auch serverübergreifende Berichte erstellen möchten, müssen die Unternehmensnamen auch serverübergreifend eindeutig sein.

Die Zeitzone verwendet der Server zum Anzeigen von Zeitstempeln und zum Auslösen von Aufträgen. Für jedes auf einem EdgeSight-Server definierte Unternehmen gilt genau eine Zeitzone. Alle Daten für das Unternehmen werden basierend auf der Tagesgrenze der Zeitzone zusammengefasst. Dies sorgt für eine größere Datenkonsistenz, wenn sich die Agentcomputer in verschiedenen Zeitzonen befinden.

Verwalten von Lizenzen

Über Citrix Lizenzserver für Windows werden EdgeSight-Agents Lizenzen bereitgestellt, mit denen diese Daten auf einen EdgeSight-Server hochladen können. Der Lizenzserver kann sich überall im Netzwerk befinden, so lange er vom EdgeSight-Webserver aus und durch die EdgeSight für XenApp-Agents erreichbar ist. Ein einzelner Lizenzserver kann von mehreren Citrix Produkten, auch mehreren EdgeSight-Servern, gemeinsam genutzt werden. Der Lizenzserver und die EdgeSight für Endpunkte-Lizenzdateien sollten nach Möglichkeit bereits vorhanden sein, bevor die Erstkonfiguration von EdgeSight vorgenommen wird.

Wichtig: Für EdgeSight für XenApp und EdgeSight für Endpunkte Agents müssen separate Lizenzen erworben werden. Dies gilt auch dann, wenn beide Agentarten mit demselben Server verknüpft sind.

Die Lizenzdatei für den EdgeSight für Endpunkte-Agent (z. B. `CESEP_*.lic`) befindet sich im Ordner "MyFiles" des Lizenzserververzeichnisses, z. B.: # `C:\Programme\Citrix\Licensing\MyFiles`.

Konfigurieren der Lizenzierung für EdgeSight für Endpunkte-Agents

Wenn die EdgeSight für Endpunkte-Unterstützung aktiviert ist, müssen Sie bei der EdgeSight Server-Installation einen Lizenzservernamen und einen Lizenzserverport eingeben. Während der anfänglichen Konfiguration mit dem Assistenten für das Setup nach der Installation können Sie die Verbindung zum Lizenzserver testen und, bei Erfolg, die Art und die Anzahl der installierten Lizenzen anzeigen.

EdgeSight Server ruft die Lizenzen für die EdgeSight für Endpunkte-Agents vom angegebenen Server ab. Sie können den Lizenzservernamen und den Lizenzserverport nach der Installation auch ändern. Wählen Sie dazu **Serverkonfiguration > Einstellungen** und bearbeiten Sie die Felder "Name des Lizenzservers" und "Lizenzserverport", wie unter "Agentunterstützung und Lizenzserver" auf Seite 61 beschrieben. Der aktuelle Lizenzservername und -port werden auf der Seite "Lizenzinformationen" angegeben (siehe dazu "Verwenden der Seite "Lizenzinformationen" zur Überwachung des Lizenzstatus" auf Seite 70).

Konfigurieren der Lizenzierung für EdgeSight für XenApp Agents

Nach der Installation erhalten die EdgeSight für XenApp Agents Standardagent-eigenschaften vom verknüpften EdgeSight-Server. Diese Eigenschaften legen fest, von welchem Lizenzserver der Agent Lizenzen abrufen soll. Folgende Lizenzserveroptionen stehen zur Verfügung:

- XenApp: Bei dieser Option wird derselbe Lizenzserver verwendet wie auf dem XenApp-Server, auf dem der Agent residiert. Dies ist die Standardeinstellung in den Agenteigenschaften "XenApp-Standard".
- Farm: Bei dieser Option wird der Lizenzserver der XenApp-Farm verwendet.
- Angepasst: Bei dieser Option werden ein explizit definierter Lizenzserver und Port verwendet.

Weitere Informationen zu Agenteigenschaften finden Sie unter "Festlegen von Agenteigenschaften" auf Seite 49 und in der Onlinehilfe im Abschnitt "Assistent für Agenteigenschaften". Was für alle Agenteigenschaften gilt, gilt auch für diese Einstellungen: Sie werden auf ganze Abteilungen angewendet und von Unterabteilungen übernommen, sofern sie nicht auf einer niedrigeren Abteilungsebene außer Kraft gesetzt werden.

Lizenzierung von EdgeSight für Endpunkte-Agents

Bei EdgeSight für Endpunkte-Agents funktioniert die Lizenzierung wie folgt:

- Bei der Konfiguration nach der Installation können Sie die Verbindung zwischen dem EdgeSight-Server und dem Lizenzserver validieren. Dieser Schritt ist optional. Der Assistent für das Setup nach der Installation kann auch ohne gültige Lizenz oder Verbindung abgeschlossen werden.
- Die Lizenzdatei, die auf dem Lizenzserver installiert ist, gibt an, wie viele EdgeSight für Endpunkte-Agents Daten auf den Server hochladen dürfen.
- EdgeSight Server kontaktiert den Lizenzserver in regelmäßigen Abständen, um zu ermitteln, ob genügend Lizenzen vorhanden sind. Wenn der Lizenzserver feststellt, dass nur noch einige wenige EdgeSight für Endpunkte-Lizenzen übrig sind, wird eine Warnungsmeldung an EdgeSight Server gesendet.
- Wenn die Anzahl der Agents die laut Lizenz zulässige Anzahl überschreitet, dürfen die Agents keine Daten auf den Server hochladen. Die Datenerfassung wird aber fortgesetzt und die Daten werden in der Agentdatenbank aufbewahrt, bis eine Optimierung erfolgt.

EdgeSight Server benötigt für jedes Endpunktgerät, das Daten liefert, eine eigene Lizenz. Beim Starten des Servers versucht EdgeSight Server, für jedes vorhandene Gerät eine Lizenz auszuchecken. Wenn nicht genügend Lizenzen für die vorhandenen Geräte verfügbar sind, werden alle verfügbaren Lizenzen ausgecheckt und den Agents in der Reihenfolge zugewiesen, in der sie Daten auf den Server hochladen, d. h., ältere Agents haben Vorrang vor neueren Agents. Nur Agents mit einer Lizenz dürfen Daten auf den Server hochladen. (Geräte, auf denen Agents ausgeführt werden, werden in der EdgeSight-Datenbank als lizenziert oder nicht lizenziert gekennzeichnet.) Wenn der Server nicht genügend Lizenzen für alle Agents auschecken konnte, versucht er dies im Abstand von jeweils einer Minute erneut. Der Nachrichtentabelle wird eine Warnungsmeldung hinzugefügt und der Serveradministrator erhält eine entsprechende E-Mail. Bei Lizenzknappheit können Sie durch Installieren neuer Lizenzen oder Löschen einer ausreichenden Anzahl bestehender Geräte Abhilfe schaffen.

Sobald der Server in der Lage ist, ordnungsgemäß zu starten, und sobald ein neues Gerät Daten an den Server liefert, checkt der Server eine Lizenz für dieses Gerät aus. Nachdem der Server eine Lizenz für das betreffende Gerät gesichert hat, kann dieses Gerät jederzeit Daten hochladen. Weitere Lizenzüberprüfungen finden nicht statt (außer im Falle des oben beschriebenen Startprozesses). Wenn ein neuer Endpunktagent keine Daten hochladen kann, weil zu wenige Lizenzen vorhanden sind, wird die Datenerfassung fortgesetzt und die Daten werden in der Agentdatenbank aufbewahrt, bis eine Optimierung erfolgt. Bei Lizenzknappheit gilt hier dasselbe wie beim Starten: Entweder Sie installieren neue Lizenzen oder Sie löschen eine ausreichende Anzahl bestehender Geräte, damit die neuen Geräte Daten hochladen können.

Wenn ein Gerät von einem Server gelöscht wird, wird die Lizenz für dieses Gerät auf dem Lizenzserver eingecheckt und steht damit zur Verwendung durch ein anderes Gerät zur Verfügung.

"Serverstart" bezieht sich hier konkret auf das Starten des Server Script Handler (RSSH). Wenn RSSH beendet wird, werden alle für diesen Server ausgecheckten Lizenzen eingecheckt und können damit so lange von anderen Servern verwendet werden, die auf denselben Lizenzserver zugreifen, bis RSSH neu gestartet wird. Dieses Verhalten muss beim Planen der erforderlichen Anzahl von Lizenzen auf jeden Fall berücksichtigt werden. Wenn Ihre Lizenzen nicht ausreichen, um alle Geräte auf allen Servern zu versorgen, könnte dies daran liegen, dass ein anderer EdgeSight-Server Lizenzen auscheckt, was zu einer Lizenzknappheit beim Starten führen würde.

Lizenzierung von EdgeSight für XenApp Agents

Bei EdgeSight für XenApp Agents funktioniert die Lizenzierung folgendermaßen:

- Die EdgeSight für XenApp Agents kommunizieren bei jeder Sitzung direkt mit dem Lizenzserver, um eine Lizenz dafür zu erhalten. Die Agents checken beim Sitzungsstart eine Lizenz auf dem XenApp-Server aus.
- Wenn keine Lizenz verfügbar ist, wird ein Verstoß protokolliert (sodass EdgeSight Server über das Problem informiert wird), die Daten werden aber während der Sitzung weiter erfasst. Wenn ein Benutzer mehrere Sitzungen auf einem oder mehreren XenApp-Servern startet, wird für alle Sitzungen dieselbe Lizenz verwendet (genau wie bei XenApp-Lizenzen).

- Die Anzahl der zulässigen Lizenzverstöße darf über dem in der Lizenz festgelegten Wert liegen, überzählige Uploads werden aber blockiert, wenn es im Lizenzüberwachungszeitraum 5 Tage hintereinander zu Lizenzverstößen kommt. (Mehrere Lizenzanzahlüberschreitungen an einem Tag zählen als ein Verstoß). Überzählige Uploads werden so lange blockiert und verworfen, bis es über einen bestimmten Zeitraum hinweg keine Verstöße mehr gegeben hat oder bis ein Lizenzupgrade durchgeführt wurde.
- Um das Installieren und Konfigurieren zu erleichtern, wird der erste Datenupload von einem XenApp-Server nicht auf Lizenzverstöße geprüft. Alle Verstöße beim ersten Hochladen von Nutzdaten werden ignoriert und verworfen.

Wichtig: Ein EdgeSight für XenApp Agent versucht, *alle* Sitzungen auf diesem XenApp-Server zu überwachen. Das Überwachen nur eines Teils der Sitzungen auf dem System ist nicht möglich. Mit anderen Worten, wenn Sie EdgeSight für XenApp für einen Teil Ihrer CCU-Basis (Concurrent User, gleichzeitige Benutzer) kaufen, müssen Sie die ungefähre Sitzungslast für den jeweiligen Server kennen und dann ermitteln, auf wie vielen Servern der Agent bereitgestellt werden muss, um diese Last bewältigen zu können. Die so ermittelte Anzahl sollte dann in die Bestimmung der Lizenzanforderungen eingehen.

Verwenden der Seite "Lizenzinformationen" zur Überwachung des Lizenzstatus

Auf der Seite "Lizenzinformationen" (**Serverkonfiguration > Lizenzierung**) können Sie die aktuelle Lizenznutzung und Angaben zum Status anzeigen. Die Seite "Lizenzinformationen" enthält die folgenden Informationen:

EdgeSight für XenApp-Lizenzstatistiken	
Aktueller Lizenzierungsstatus	Gibt an, ob das System ordnungsgemäß lizenziert ist. Das System ist dann lizenzgemäß, wenn die zulässige Anzahl von Tagen mit Lizenzverstößen nicht überschritten wurde. Es gibt die folgenden Lizenzstatus: Lizenzgemäß: Alle vorhandenen Geräte, die diesem Server Bericht erstatten, konnten Lizenzen abrufen. Warnung: Die Anzahl der Lizenzen hat in diesem Überwachungszeitraum die maximal zulässige Anzahl von Lizenzen überschritten. Im Feld "Tage mit Lizenzverstoß" werden die Anzahl der Tage mit Lizenzverstoß und die Server angezeigt, von denen der Lizenzverstoß gemeldet wird. Mit Verstoß: Die Anzahl der verwendeten Lizenzen lag während dieses Überwachungszeitraums für mindestens 5 Tage über der zulässigen Anzahl von Lizenzen.
Kulanzzeitraum für neues Gerät	In diesem Zeitraum werden Nutzdaten, die von Agents mit Lizenzverstößen hochgeladen werden, nicht abgelehnt. Dem EdgeSight-Administrator wird eine Warnungs-E-Mail gesendet und auf der Seite "Nachrichten" wird die Nachricht angezeigt, dass ein Lizenzverstoß vorliegt. Mit dieser Funktion können Administratoren Probleme mit anfänglichen Konfigurationen beheben.
Tage mit toleriertem Lizenzverstoß	Gibt die Anzahl der Tage im Überwachungszeitraum an, an denen die Anzahl der verwendeten Lizenzen über der gewährten Anzahl der Lizenzen liegen darf. Wenn die Anzahl der Tage mit Lizenzverstöen die Grenze von fünf (5) Tagen überschreitet, werden Uploads blockiert.
Lizenzverstoßüber-wachungszeitraum	Gibt die Anzahl der Tage an, für die Lizenzverstöße verfolgt werden.
Tage mit Lizenzverstoß	Gibt die aktuelle Anzahl der Tage im Überwachungszeitraum an, an denen die Anzahl der verwendeten Lizenzen über der gewährten Anzahl der Lizenzen liegen darf. Erweitern Sie dieses Element, um die Daten des Lizenzverstoßes und die Namen der Server anzuzeigen, die den Verstoß gemeldet haben.

Endpunktlizenzstatistiken	
Aktueller Lizenzierungsstatus	Gibt an, ob das System ordnungsgemäß lizenziert ist. Es gibt die folgenden Lizenzstatus: Lizenzgemäß: EdgeSight Server konnte Lizenzen für alle vorhandenen Geräte abrufen, die diesem Server Bericht erstatten. Fehler: EdgeSight Server konnte nicht für alle auf diesem Server vorhandenen Geräte Lizenzen abrufen. EdgeSight versucht weiterhin, für alle Geräte Lizenzen zu abzurufen. Beendet: Der License Manager wird derzeit nicht ausgeführt. Möglicherweise wird auch eine Nachricht angezeigt, dass der Server gerade Lizenzen abruft. Wenn der Server beim Start nicht für alle registrierten Endpunktgeräte Lizenzen abrufen kann, wird eine Meldung angezeigt und der Server versucht alle 15 Minuten erneut, Lizenzen abzurufen. Sie können es sofort erneut versuchen, indem Sie auf die Schaltfläche **Endpunktlizenzierung aktualisieren** klicken. Diese Schaltfläche wird nur angezeigt, wenn beim Start Fehler beim Abrufen von Lizenzen auftreten.
Lizenzierte Geräte auf diesem Server	Gibt die Anzahl der Endpunktlizenzen an, die derzeit von Agents verwendet werden, die Berichte an diesen Server senden. Diese wird im Vergleich zur Gesamtzahl der Agents angezeigt, die auf dem Server registriert sind. Wenn beispielsweise 500 Agents auf dem Server registriert sind und 487 Agents derzeit Lizenzen verwenden, wird in diesem Feld "487 von 500" angezeigt.
Lizenzserver	Gibt den Namen und die Portnummer des Lizenzservers an, von dem EdgeSight Endpunktagentlizenzen abruft. Der Server und der Port werden während der Installation angegeben und können anschließend auf der Seite "Einstellungen" geändert werden.
Installierte Lizenzen (insgesamt)	Gibt die Gesamtzahl der Lizenzen für Endpunktagents laut installierter Lizenzdatei an.
Verfügbare Lizenzen	Gibt an, wie viele Lizenzen für Endpunktagents verfügbar sind.
Ablaufdatum	Gibt das Datum an, an dem die Lizenzdatei abläuft. Vor dem Ende der Ablauffrist für die Lizenzdatei erhalten Sie eine Benachrichtigung.

Verwalten von Authentifizierungsprovidern

Authentifizierungsprovider sorgen dafür, dass sich nur berechtigte Benutzer auf einem EdgeSight-Server anmelden können. Der erste Schritt beim Erstellen eines neuen Benutzers besteht im Auswählen eines Authentifizierungsproviders, bei dem der Benutzername und das Kennwort überprüft werden.

Beim Installieren von EdgeSight Server wird auch ein Standardauthentifizierungsprovider (E-Mail) bereitgestellt. Der Standard-Authentifizierungsprovider kann weder bearbeitet noch gelöscht werden. Er verwendet die E-Mail-Adresse als Benutzernamen. Die E-Mail-Adresse für einen Benutzer legen Sie bei dessen Erstellung fest. Anschließend wird eine E-Mail mit einer Erläuterung des Anmeldevorgangs und dem temporären Kennwort an den Benutzer gesendet. Beim ersten Anmelden wird der Benutzer aufgefordert, sein Kennwort zu ändern.

Sie können neue Authentifizierungsprovider erstellen, die für die Sicherheits- und Anmeldefunktionen Active Directory (AD) verwenden. Stellen Sie vor dem Erstellen eines neuen Providers sicher, dass der LDAP-Pfad für den AD-Authentifizierungsprovider verfügbar ist.

Zum Einrichten der Active Directory-Integration mit EdgeSight müssen Sie einen Active Directory-Authentifizierungsprovider einrichten. Stellen Sie zuvor sicher, dass Sie den LDAP-Pfad zu diesem Authentifizierungsprovider zur Hand haben.

1. Melden Sie sich an der EdgeSight Server Console an.
2. Wählen Sie im Navigationsbereich **Serverkonfiguration > Authentifizierung**. Die Seite "Authentifizierungskonfiguration" wird geöffnet. Beachten Sie, dass der Provider "E-Mail" bereits aufgeführt wird.
3. Klicken Sie auf **Neuer Provider**, um den Assistenten für Authentifizierungsprovider zu starten.
4. Klicken Sie auf **Hilfe** und führen Sie die im Abschnitt zum Assistenten für Authentifizierungsprovider angezeigten Anweisungen aus.

Nach dem Hinzufügen eines Authentifizierungsproviders und dem Einrichten von Rollen müssen Sie noch Benutzer und/oder Gruppen einrichten. Sie können in Active Directory mehrere Gruppen erstellen, z. B. eine EdgeSight-Administratorengruppe und eine EdgeSight Console-Benutzergruppe, um sich so die Verwaltung zu erleichtern.

1. Wählen Sie im Navigationsbereich **Unternehmenskonfiguration > Sicherheit > Benutzer**, um die Seite "Benutzer verwalten" zu öffnen.
2. Klicken Sie auf **Neuer Benutzer**, um den Assistenten zum Hinzufügen von Benutzern zu starten.
3. Klicken Sie auf **Hilfe** und führen Sie die im Abschnitt "Assistent zum Hinzufügen von Benutzern" angezeigten Anweisungen aus.

4. Testen Sie den neu eingerichteten Benutzer bzw. die neu eingerichtete Gruppe. Melden Sie sich beim EdgeSight-Server ab und wieder an. Auf der Anmeldeseite wird jetzt die Dropdownliste **Provider** angezeigt. Der Benutzer oder das Gruppenmitglied wählt den entsprechenden Provider aus und meldet sich dann mit seiner Domänenbenutzer-ID und seinem Kennwort an.

Konfigurieren der Verbindung zu Reporting Services

Zum Generieren und Anzeigen von EdgeSight-Berichten muss Microsoft SQL Server Reporting Services installiert und konfiguriert sein. Ausführliche Anleitungen zum Installieren und Konfigurieren von Reporting Services und der zugehörigen Software finden Sie unter *Konfigurieren von Reporting Services für Citrix EdgeSight*.

Nach dem Installieren und Konfigurieren von Reporting Services müssen Sie die Verbindung von EdgeSight Server zum Berichtserver konfigurieren. Wählen Sie **Serverkonfiguration > Reporting Services > URL des Berichtservers**, um den Berichtserver, die Anmeldedaten für den Zugriff auf den Berichtserver und die Datenquelle sowie die standardmäßigen Berichts- und Zeitplanoperationen festzulegen. Weitere Informationen dazu finden Sie in der Onlinehilfe im Abschnitt "Einstellungen für Berichtserver".

Verwalten von Reporting Services-Zeitplänen

Mit den Reporting Services-Zeitplänen und der Abonnementfunktion können Sie das Generieren von Berichten für die Verteilung an die Benutzer automatisieren. Wenn ein Administrator oder Benutzer ein Abonnement für einen Bericht erstellt, muss er einen zugehörigen Zeitplan auswählen. Wählen Sie **Serverkonfiguration > Reporting Services > Zeitpläne**, um vorhandene Zeitpläne zu verwalten und neue Zeitpläne zu erstellen. Weitere Informationen dazu finden Sie in der Onlinehilfe im Abschnitt "Reporting Services-Zeitpläne".

In manchen Fällen, z. B. Wochen mit Feiertagen oder unternehmensinternen werkfreien Tagen, ist es unter Umständen erforderlich, Berichtzeitpläne anzuhalten, damit die entsprechenden Berichte nicht generiert werden.

Das Löschen von Zeitplänen sollte nur nach sorgsamer Überlegung erfolgen. Wenn der gelöschte Zeitplan mit einem Bericht verknüpft ist, wird dieser Bericht nicht mehr generiert. Außerdem führen Abonnements, die den gelöschten Zeitplan verwenden, nicht zum Verteilen des Berichts.

Verwalten der Datenbank

In diesem Abschnitt wird beschrieben, wie Sie die EdgeSight-Datenbank, einschließlich des Optimierungszeitplans, effektiv verwalten können.

Konfigurieren von Datenuploads

Sie können (über **Serverkonfiguration > Datenwartung > Uploadkonfiguration**) festlegen, was für Leistungs- und Verfügbarkeitsdaten auf den Server hochgeladen werden. Auf diese Weise können Sie die EdgeSight Server-Leistung optimieren, indem Sie Datenuploads begrenzen, um die in Ihrem Unternehmen verwendeten Daten widerzuspiegeln.

Das Hochladen von XenApp-Umgebungsauslastungsdaten ist standardmäßig deaktiviert und sollte nur aktiviert werden, wenn Sie den Bericht "Umgebungsauslastung" verwenden wollen, in dem diese Daten enthalten sind. Je nach Anzahl der Sitzungen für die Gruppe oder das Gerät können die zum Generieren dieser Berichte verwendeten Daten zu einem signifikanten Anwachsen Ihrer EdgeSight-Datenbank führen. Häufig bietet es sich daher an, die Datenerfassung nur so lange zu aktivieren, wie es erforderlich ist, und sie dann wieder zu deaktivieren.

Datenbankoptimierung

EdgeSight erfasst eine breite Palette an Leistungs-, Verfügbarkeits- und Nutzungsdaten zu Endbenutzersystemen, Anwendungen, Benutzersitzungen und dem Netzwerk. Die EdgeSight-Agents sammeln die Daten von den Systemen und laden sie auf einen EdgeSight-Server hoch. Je nach Anzahl der Endpunkt- und XenApp-Systeme, der Anzahl der Anwendungen und der Netzwerkaktivität können die Datenbanken ohne eine sorgfältige Verwaltung schnell sehr groß werden. Das wichtigste Mittel bei der Datenbankverwaltung ist die Optimierung.

Bei der Optimierung werden in regelmäßigen Abständen ältere Daten aus der Datenbank gelöscht, um Platz für neue Daten zu schaffen. Diese Optimierung ist für die Aufrechterhaltung einer effizienten Datenbankarbeit ganz entscheidend. Ein effektiver Optimierungszeitplan hält die Größe der Datenbank unter Kontrolle und hilft, eine akzeptable Leistung sicherzustellen. Gleichzeitig sorgt er dafür, dass ausreichend Daten für die Geschäftsabläufe zur Verfügung stehen.

Das folgende Beispiel zeigt, wie sich Datenbankoptimierungseinstellungen auf die Größe der EdgeSight Server-Datenbank auswirken. Sie haben EdgeSight-Agents auf 2500 Endbenutzergeräten bereitgestellt. Die Geräte führen in dem Zeitraum, in dem Netzwerkdaten aufbewahrt werden, durchschnittlich 50 Prozesse aus und greifen im Schnitt auf 100 Websites zu. Die Agents erfassen pro Werktag 12 Stunden lang Daten. Wenn der Parameter für die Datenbank-optimierungsparameter für die Netzwerkstatistik von 7 in 14 Tage geändert wird, vergrößert sich die Datenbank um ca. 40 %, was ungefähr dieselbe Wirkung hat, als wenn der Bestand verwalteter Geräten um 1000 Stück erhöht wird.

Optimierungszeitplan

EdgeSight verfügt über eine verteilte Struktur, wobei sich auf jedem verwalteten Gerät EdgeSight-Agentdatenbanken befinden, die in eine einzelne EdgeSight Server-Datenbank hochgeladen werden. Die Einstellungen für die Datenaufbewahrung für die Agentdatenbanken werden in den Agenteigenschaften festgelegt und entsprechend ihrer Abteilungsmitgliedschaft auf die Geräte angewendet.

Der Optimierungszeitplan für die Serverdatenbank wird im Rahmen der Serverkonfiguration festgelegt. Im Serveroptimierungszeitplan können Sie datentypabhängig angeben, wie lange die Daten aufbewahrt werden sollen. Auf diese Weise können Daten zum Aufspüren von Trends, wie z. B. Leistungsdaten, länger aufbewahrt werden als Daten, die schnell veralten, wie z. B. Daten zu Echtzeitwarnungen.

Die Standardwerte für die Optimierung der Serverdatenbank sind für die meisten Installationen vollkommen ausreichend. Sie können daher zunächst die Standardwerte verwenden und diese dann nach und nach an den Benutzerbedarf und die Systemleistung anpassen. Wenn Sie mehr Daten aufbewahren möchten, sollten Sie zum Aufbewahren von Verlaufsdaten das Erstellen eines Archivberichts oder den Einsatz von Data Warehousing in Erwägung ziehen, anstatt die Optimierungskonfiguration zu lockern. Weitere Informationen zur Verwendung von EdgeSight-Daten zu Analyse- und Dokumentationszwecken finden Sie in der *Citrix EdgeSight-Benutzerdokumentation*.

Optimieren der Serverdatenbank

Wählen Sie **Serverkonfiguration > Datenwartung > Optimierung**, um den Optimierungszeitplan für die Datenbank zu bearbeiten (siehe "Optimierungskonfiguration" in der Onlinehilfe). Die Tabelle "Optimierung" enthält die folgenden Informationen:

- **Berichtsdaten:** Gibt den Typ der zu optimierenden Daten an.
- **SQL Server-Tabelle:** Gibt die Datenbanktabelle an, in der die Daten gespeichert werden.
- **SQL Server-Ansicht:** Gibt die SQL-Ansichten an, die mit der Datenbanktabelle verknüpft sind, in der die Daten gespeichert werden. In diesen Ansichten können Berichte bearbeitet und angepasste Berichte erstellt werden. Eine Definition der einzelnen Ansichten finden Sie in der Onlinehilfe.
- **Tage für Optimierung:** Gibt an, wie lange die Daten des ausgewählten Typs aufbewahrt werden, bevor eine Optimierung erfolgt.

Meistens ist der Optimierungszeitplan so ausgelegt, dass die Daten einen Monat lang aufbewahrt werden. Daten zur Anwendungsnutzung werden 90 Tage lang aufbewahrt, da in vielen Umgebungen die Anwendungsnutzung zur Erstellung von Lizenz- und Compliance-Berichten nachverfolgbar sein muss. Im Gegensatz dazu werden Daten zur Netzwerknutzung aufgrund der großen Datenmengen und ihrer Kurzlebigkeit nur 10 Tage lang aufbewahrt.

Bei der Erarbeitung einer Optimierungsstrategie für die einzelnen Datentypen sollte berücksichtigt werden, wie schnell die Daten ab dem Zeitpunkt ihrer Erfassung ihre Bedeutung verlieren und auch wie viele Daten eines bestimmten Typs durchschnittlich in einem gegebenen Zeitraum erfasst werden. So sind z. B. die Daten in der Tabelle `alert_incoming` nur kurze Zeit von Bedeutung. Echtzeitwarnungen haben die Aufgabe, auf kritische Probleme aufmerksam zu machen, die durch entsprechende Maßnahmen innerhalb kurzer Zeit gelöst werden können, wie z. B. Abstürze missionskritischer Anwendungen oder Netzwerkausfälle. Aufgrund dieser Eigenschaft und weil Verlaufsdaten mit Warnungen aufbewahrt werden, werden Daten zu Echtzeitwarnungen sehr strikt optimiert.

Wichtig ist es sicherzustellen, dass der Optimierungszeitplan berücksichtigt, ob Data Warehousing stattfindet oder Berichte archiviert werden. Wenn Daten seltener übertragen als optimiert werden, kann es zu Datenverlust kommen. Genauso gilt, dass bei Zeitplänen für die Berichtsarchivierung der Optimierungszeitplan zu berücksichtigen ist, damit in den Verlaufsberichten keine Lücken entstehen.

Den Status der Optimierungsaufträge können Sie im Optimierungsprotokoll (**Serverstatus > Optimierungsprotokoll**) überwachen. Das Protokoll enthält die folgenden Informationen:

- **Datenbereich:** Gibt den Datentyp an, für den die Optimierung ausgeführt wurde.
- **Auftragsname:** Gibt den Namen des ausgeführten Optimierungsauftrags an, z. B. core_groom_instance.
- **Auftragsstatus:** Gibt an, in welchem Status sich der Auftrag nach Fertigstellung befindet, z. B. "Wartungsauftrag erfolgreich abgeschlossen".
- **Startzeit:** Gibt den Zeitpunkt an, zu dem der Optimierungsauftrag gestartet wurde.
- **Dauer:** Gibt an, wie lange die Ausführung des Optimierungsauftrags gedauert hat. Zu beachten ist, dass bei kleineren Datenbanken für Optimierungsaufträge als Dauer möglicherweise der Wert 0 angezeigt wird.

Verwalten von Wartungsaufträgen

Neben der Optimierung gibt es noch eine ganze Reihe anderer Wartungsarbeiten, die ein EdgeSight-Server auszuführen hat. So müssen z. B. Datenuploads verarbeitet sowie der Inhalt von Caches und temporären Speicherbereichen gelöscht werden. Jeder Auftrag ist mit einem der folgenden Zeitpläne verknüpft: "Fünfzehn Minuten" oder "Nachts". Beim Zeitplan des Typs "Fünfzehn Minuten" wird der jeweilige Auftrag alle 15 Minuten ausgeführt, wenn der EdgeSight-Server in Betrieb ist, und kann nicht konfiguriert werden. Beim Zeitplan des Typs "Nachts" wird der jeweilige Auftrag einmal pro Nacht ausgeführt, wobei die Startzeit nach Wunsch konfiguriert werden kann. Standardmäßig ist als Startzeit 00:05 Uhr Serverzeit festgelegt. Auf diese Weise wird der Auftrag zu einer Zeit ausgeführt, zu der die wenigsten Benutzer aktiv sind. Der folgenden Tabelle können Sie entnehmen, auf welcher Konsolenseite die einzelnen Wartungsaufträge verwaltet werden können.

Konsolenseite	Vorgänge
Serverkonfiguration > Datenwartung > Aufträge	Anzeigen von Zeitplänen für Aufträge, Bearbeiten der Startzeit für den Zeitplan "Nachts" und manuelles Ausführen von Aufträgen, die mit Zeitplänen verknüpft sind
Serverstatus > Auftragsstatus	Feststellen, wann die Aufträge zum letzten Mal ausgeführt wurden und wie ihr Status nach Fertigstellung lautet. Sie können sich hier auch die Gesamtdauer aller Aufträge anzeigen lassen und herausfinden, wie lange die einzelnen Aufträge bei ihrer letzten Ausführung gedauert haben.
Serverstatus > Auftragsprotokoll	Anzeigen der Ausführungshistorie für die einzelnen Aufträge einschließlich Ergebnis, Dauer und Startzeit

Umgang mit nicht verwalteten Geräten

Nicht verwaltete Geräte sind Systeme, auf denen ein EdgeSight-Agent ausgeführt wird, die aber nicht mit einem Unternehmen oder einer Abteilung verknüpft sind. Der Agent kann mit dem Server kommunizieren und in die Liste der nicht verwalteten Geräte aufgenommen werden, sofern für ihn bei der Installation ein gültiger Server und Port angegeben wurde. Dafür, dass Geräte nicht verwaltet sind, kann es folgende Gründe geben:

- Die Informationen zum Unternehmen, die der Agent beim Registrieren auf dem Server bereitgestellt hat, stimmen mit keinem der vorhandenen Unternehmen überein.
- Die Einstellung **Agents automatisch registrieren** ist deaktiviert. (Weitere Informationen dazu finden Sie unter "Agentregistrierungseinstellungen" auf Seite 27.)
- Auf dem Gerät wurde eine Datenbank beschädigt und eine Wiederherstellung war nicht möglich.

Zum Überwachen der Anzahl nicht verwalteter Geräte können Sie entweder die Seite "Systemstatus" öffnen oder aber **Servereinstellungen > Konfiguration > Nicht verwaltete Geräte** wählen. Auf der Seite "Nicht verwaltete Geräte" können Sie ein Gerät in ein Unternehmen oder eine Abteilung verschieben. Geräte, auf denen EdgeSight für XenApp 5.0-Agents ausgeführt werden, können nur in PS-Farmen-Abteilung verschoben werden. Alle anderen Geräte können in die Endpunkte-Abteilung verschoben werden. Bei Agents, die zuvor auf dem Server registriert waren, wird im Feld **Registrierte Org.** die Abteilung angezeigt, in die das Gerät zuletzt Daten hochgeladen hat.

Auf nicht verwalteten Geräten erfasst der EdgeSight-Agent Daten und lädt sie zum Server hoch. Er erscheint jedoch nicht in historischen oder Echtzeitberichten. Die Daten werden ebenfalls der Optimierung unterzogen. Wenn Geräte für längere Zeit nicht verwaltet werden, kann dies also zum Verlust von Daten führen. Im Feld **Letzter Upload** können Sie herausfinden, wann der Agent auf dem Gerät zum letzten Mal mit dem Server kommuniziert hat.

Anzeigen des Status des Agentdatenbankbrokers

Auf den Konfigurationsseiten im Ordner "Pool-Datenbankbroker" (Pools, Agentdatenbankserver, Brokerverlauf) werden nur Daten angezeigt, wenn der EdgeSight-Server als Datenbankbroker für EdgeSight für Endpunkte Agents fungiert, die auf virtuellen Desktops in gepoolten Umgebungen installiert sind. Obwohl die Datenbankbroker-Komponenten Teil aller EdgeSight Server-Installationen sind, werden sie nur verwendet, wenn der Server während der Installation von Agentdatenbankserver und EdgeSight-Agent als Datenbankbroker angegeben wird. Eine Beschreibung der verschiedenen für die Überwachung virtueller Desktops erforderlichen Komponenten finden Sie unter "EdgeSight-Komponenten für die Überwachung virtueller Desktops" auf Seite 11.

Auf diesen Seiten wird der Status von Agentdatenbankservern, Pools und Geräten (in diesem Fall virtuelle Desktops, auf denen EdgeSight-Agents ausgeführt werden) angezeigt. Auf diesen Seiten werden größtenteils Wartungsaufgaben durchgeführt, z. B. Löschen nicht verwendeter Pools oder veralteter Registrierungsinformationen für Agentdatenbankserver. Aktionen, die direkte Auswirkungen auf Ihre Umgebung haben, sind das Neuverteilen von Pools und Aktivieren/Deaktivieren von Agentdatenbankservern.

Anzeigen des Poolstatus und Neuverteilen von Pools

Auf der Seite "Datenbankbrokerpools" (**Konfigurieren > Serverkonfiguration > Pool-Datenbankbroker > Pools**) werden Informationen über Pools (benannte Gruppen virtueller Desktops) angezeigt. Der Poolname entspricht dem XenDesktop-Desktopgruppennamen. Auf dieser Seite können Sie außerdem Pools neu verteilen oder löschen.

Mit der Funktion "Neu verteilen" können Sie eine Umverteilung der Agents auf den Datenbankservern erzwingen. Die Agents werden nicht sofort neu verteilt; die Neuverteilung findet über einen längeren Zeitraum statt, in dem virtuelle Desktops heruntergefahren und wieder gestartet werden.

Achtung: Wenn Sie Agents in einem Pool über mehrere Datenbankserver neu verteilen, führt dies zum Verlust von auf diesen Servern gespeicherten EdgeSight-

Agentdaten. Führen Sie keine manuelle Neuverteilung durch, wenn Sie Agentdaten aufbewahren müssen.

Das Löschen von Pools ist eine Wartungsaufgabe, die nur dann durchgeführt werden sollte, wenn alle mit einem Pool verknüpften Agentdatenbankserver gelöscht wurden. Weitere Informationen über die Neuverteilung und das Löschen von Pools finden Sie in der Onlinehilfe im Abschnitt "Pools".

Anzeigen des Datenbankserverstatus

Auf der Seite "Agentdatenbankserver" (**Konfigurieren > Serverkonfiguration > Pool-Datenbankbroker > Datenbankbrokerserver**) wird der aktuelle Serverstatus angezeigt und Sie können Aktionen für alle Agentdatenbankserver vornehmen, die bei den Datenbankbroker-Komponenten von EdgeSight Server registriert sind. Sie können Server aktivieren/deaktivieren und löschen.

Wenn ein Datenbankserver gewartet werden muss oder ein Problem aufgetreten ist, können Sie den Datenbankserver deaktivieren. Deaktivieren eines Servers bedeutet, dass die Datenbankbrokerkomponenten von EdgeSight Server den Server nicht mehr neuen Agents zuweisen. Die Agents, die den Datenbankserver bereits verwenden, speichern weiterhin Daten in der Datenbank. Nachdem die Wartung abgeschlossen ist oder das Problem gelöst wurde, können Sie den Server aktivieren, damit er als Broker für Agents zur Verfügung steht.

Beim Löschen eines Agentdatenbankservers werden nur die in der EdgeSight Server-Datenbank gespeicherten Registrierungsdaten gelöscht, z. B. Name des Agentdatenbankservers, Port und Poolzuordnung. Hiermit soll es Ihnen ermöglicht werden, veraltete Registrierungsdaten von Servern zu entfernen, die deinstalliert oder einem anderen EdgeSight-Server zugeordnet wurden.

Weitere Informationen über Serverstatus, Aktivieren/Deaktivieren und Löschen von Servern finden Sie in der Onlinehilfe im Abschnitt "Agentdatenbankserver".

Anzeigen des Brokerverlaufs

Auf der Seite "Brokerverlauf" (**Konfigurieren > Serverkonfiguration > Pool-Datenbankbroker > Brokerverlauf**) werden Statusmeldungen für EdgeSight-Agentdatenbankserver, Pools und Geräte angezeigt. Sie können die Meldungsliste nach Server, Pool oder Gerät filtern, wobei Sie eine chronologische Liste für die ausgewählte Komponente erhalten. Die meisten Meldungen haben Informationscharakter. Es werden aber auch Fehler angezeigt für Agents, die keine Verbindung zum Datenbankserver herstellen können. Beachten Sie, dass lange Fehlermeldungen nach ungefähr 512 Zeichen abgeschnitten werden. Weitere Informationen über einzelne Spalten in der Tabelle "Brokerverlauf" finden Sie in der Onlinehilfe im Abschnitt "Brokerverlauf".

Fehlerbehebung bei Datenbankbrokerproblemen

Sie können auf der Registerkarte **Agentdatenbankbroker** unter **Serverkonfiguration > Einstellungen** detaillierte Protokollierung für die Fehlerbehebung von Brokerproblemen aktivieren (siehe "Protokollierung für Agentdatenbankbroker" auf Seite 62).

Agents können bei der Installation so konfiguriert werden, dass sie Datenbankverbindungsinformationen vom EdgeSight-Server, der als Datenbankbroker fungiert, abrufen. Wenn keine Verbindung zur Datenbank hergestellt werden kann, wird der Agent heruntergefahren und schreibt Fehlerinformationen in die lokale Protokolldatei `SYS_EVENT_TXT.TXT`. Wenn der Dateiüberwachungsdienst auf dem Agent ordnungsgemäß ausgeführt wird, wird eine Kopie dieser Datei auf die Dateifreigabe für Agentdaten kopiert. Wenn das Problem darin besteht, dass für den Datenbankbroker ein falscher Pfad angegeben wurde, können Sie die Konfigurationseinstellungen mit dem Systemsteuerungs-Applet Citrix System Monitoring Agent ändern. Sie müssen diese nderungen auf dem Basis-Image vornehmen, damit sie an alle Desktops weitergegeben werden. Weitere Informationen zum Installieren und Konfigurieren von Agents in gepoolten Umgebungen finden Sie unter *Citrix EdgeSight-Installationsdokumentation*.

Anzeigen von und Reagieren auf Servernachrichten

Auf der Seite "Nachrichten" (**Serverstatus > Nachrichten**) werden Status- und Ereignisnachrichten für EdgeSight Server und für Geräte angezeigt, auf denen EdgeSight-Agents ausgeführt werden. Sie können die Liste der Nachrichten nach Nachrichtentyp ("Alle Typen", "Fehler", "Warnung", "Information", "Neues Gerät" oder "Aktive Überwachung") und nach Unternehmen ("Alle Unternehmen", "Kein Unternehmen angegeben" oder konkretes Unternehmen) filtern.

Verwalten von Serverskripts

Auf der Seite "Server Script Host" (**Serverstatus > Server Script Host**) wird der Status der Dienste auf dem EdgeSight-Server angezeigt. Zu diesen Diensten gehören grundlegende Serverfunktionen, wie z. B. die Verarbeitung von Warnungen, Nutzdaten und Absturzdateien sowie Wartungsfunktionen, wie z. B. das Bereinigen von temporären Ordnern und Ordnern mit Absturzberichten. Jeder Dienst ist mit einer Protokolldatei verknüpft, die beim Aufspüren von Problemen mit Serveroperationen hilfreich sein kann. Sie können Dienste auch starten und beenden, wobei dies in der Regel nur auf Anweisung des technischen Supports von Citrix erfolgen sollte.

Verwenden von EdgeSight in gemischten Umgebungen

In diesem Kapitel wird beschrieben, welche Daten erfasst und angezeigt werden, je nach der Version des EdgeSight-Agents und der Version von XenApp oder Presentation Server, die überwacht wird.

Verfügbarkeit von EdgeSight-Features nach Agentunterstützungs-Einstellung

Dieser Abschnitt enthält Informationen darüber, welche Features angezeigt und welche Daten gesammelt werden, basierend auf den Agentunterstützungs-Einstellungen (Registerkarte **Konfigurieren > Serverkonfiguration > Einstellungen**). Die Serverfeatures sind unterteilt nach den Registerkarten, auf denen sie in der EdgeSight Server Console angezeigt werden, oder nach Featuretyp, z. B. Warnungen. Ein **X** zeigt an, ob das Feature oder die Daten vorhanden sind. Wenn die Spalte leer ist, stehen das Feature bzw. die Daten nicht zur Verfügung.

Beachten Sie, dass die Agentunterstützungs-Einstellungen nur die Anzeige von Daten in der Konsole steuern; die Datensammlung durch Agenten wird davon nicht beeinflusst.

EdgeSight bietet folgende Agenttypen:

- EdgeSight für Endpunkte: Endpunkt-Agents bieten Überwachungs- und Datensammlungsfunktionen für Endpunktgeräte.
- EdgeSight für virtuelle Desktops Agent: Agents für virtuelle Desktops überwachen virtuelle Desktops, die auf XenDesktop 4.0 basieren. Zusätzlich zur Überwachung von System-, Anwendungs- und Netzwerkleistung sammelt sie ICA-Kanal-Daten einschließlich von XenDesktop-Multimedialeistungsindikatoren, Endbenutzererlebnisdaten und sendet Warnungen über die XenDesktop-Sitzungsleistung. Beachten Sie, dieser Agent nicht den Desktop Delivery Controller (DDC) überwacht.

- EdgeSight für XenApp, Standard: Standard-Agents bieten die Ressourcenverwaltungsfunktionen, die Teil von XenApp Enterprise Edition sind. Hierfür ist nur erforderlich, dass Sie eine XenApp Enterprise-Lizenz auf Ihrem Citrix Lizenzserver haben.
- EdgeSight für XenApp, Erweitert: Erweiterte Agents bieten den vollen Funktionsumfang von EdgeSight für XenApp. Hierfür benötigen Sie entweder eine XenApp Platinum Edition-Lizenz oder eine EdgeSight für XenApp-Lizenz auf Ihrem Citrix Lizenzserver.

Registerkarte "Überwachen"

Feature	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Farmüberwachung		X	X	X
Warnungskonsole	X	X	X	X
Dashboard	X	X	X	X
Warnungsliste	X	X	X	X

Registerkarte "Fehlerbehebung"

Menü	Feature	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Fehlerbehebung	Benutzerfehlersuche		X	X	
	Gerätefehlersuche	X	X	X	X
	Geräte-verfolgungsroute	X		X	X
	Geräteprozessliste	X	X	X	X
	EdgeSight Server suchen	X	X	X	X

Menü	Feature	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Echtzeitberichte	Geräteübersicht:	X	X	X	X
	Warnungsliste	X	X	X	X
	Systemleistung:	X	X	X	X
	Systemvergleich	X	X	X	X
	Netzwerkleistung:	X		X	X
	XenApp-Benutzerübersicht			X	
	XenApp-Übersicht		X	X	
	Benutzerdefinierte Leistungsindikatoren	X	X	X	X

Registerkarte "Planen und Verwalten"

Feature	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Übersicht	X	X	X	X
Geräteübersicht:	X	X	X	X
Netzwerkübersicht	X		X	X
Netzwerkübersicht nach Standort	X		X	X
Netzwerktransaktionsübersicht	X		X	X
XenApp-Übersicht		X	X	
XenApp-Benutzerübersicht			X	
Prozessleistungsübersicht nach Prozess	X	X	X	X
Prozessstabilitätsübersicht nach Prozess	X		X	X
Prozessübersicht	X	X	X	X
Benutzerübersicht für eine Benutzergruppe			X	X
XenDesktop-Übersicht				X
XenDesktop-Benutzerübersicht				X

Registerkarte "Durchsuchen"

Hinweis: Die Berichte "Sitzungen erstellt" und "Sitzungen erstellt für eine Benutzergruppe" wurden umbenannt in "Daten zu Benutzeranmeldungen" und "Daten zu Benutzeranmeldungen für eine Benutzergruppe", um deutlicher zu machen, was für Daten in den Berichten enthalten sind. Einige Berichte wurden auch umbenannt, um Presentation Server mit XenApp zu ersetzen.

Berichtsname	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Warnungen	X	X	X	X
Anwendungsreaktionsfehler			X	
Anwendungsreaktionszeit			X	
Anwendungsreaktionszeit für einen Test			X	
Anlagenänderungen	X	X	X	X
Anlagen eines Geräts	X	X	X	X
CPU-Nutzungsverwaltung		X	X	
Gerätearchiv	X	X	X	X
Geräteübersicht:	X	X	X	X
Umgebungsnutzung		X	X	X
Fehlerarchiv	X	X	X	X
Ereignisprotokollwarnungen	X	X	X	X
Ereignisprotokollwarnungen für eine Benutzergruppe	X	X	X	X
Hardwarewarnungen	X		X	X
Hardware-Anlagenänderungen	X	X	X	X
HDX MediaStream-E/A				X
HDX Plug-n-Play-E/A				X
ICA-Audio-E/A			X	X
ICA-Client-Version			X	X
ICA-Laufwerks-E/A			X	X
ICA-Drucker-E/A			X	X
Komprimierung der ICA-Sitzung			X	X
ICA-Sitzungs-E/A			X	X

Berichtsname	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
ICA-Sitzungs-Latenz			X	
ICA-Sitzungs-Latenz für eine Benutzergruppe			X	
Roundtrip-Zeit für ICA-Sitzung			X	X
Archiv für Roundtrip-Zeit für ICA-Sitzung			X	X
Roundtrip-Zeit für ICA-Sitzung für eine Benutzergruppe			X	X
ICA-Sitzungs-Datenverkehr			X	X
ICA-Sitzungs-Datenverkehr für eine Benutzergruppe			X	X
ICA-Video-E/A			X	X
Verfügbarkeit des IMA-Dienstes		X	X	
IMA-Dienststatus		X	X	
Archiv für Netzwerkverbindung	X		X	X
Netzwerkübersicht	X		X	X
Netzwerkübersicht nach Standort	X		X	X
Archiv für Netzwerktransaktion	X		X	X
Netzwerktransaktionsübersicht	X		X	X
Neue Prozesse	X	X	X	X
Neue Standorte	X		X	X
Portnetzwerkverzögerung	X		X	X
Netzwerk-Roundtrip-Zeit für Port	X		X	X
Portnetzwerkvolumen	X		X	X
Portwebfehler	X		X	X
Prozess-CPU	X	X	X	X
Kumulative CPU für Prozess	X	X	X	X
Prozessfehler	X		X	X

Berichtsname	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Prozessfehler für eine Benutzergruppe	X		X	X
Prozessorinterne Prozessfehler	X		X	X
Prozessausfälle für eine Benutzergruppe	X		X	X
Prozessspeichernutzung	X	X	X	X
Prozessnetzwerkverzögerung	X		X	X
Prozessnetzwerkvolumen	X		X	X
Warnungen "Prozess reagiert nicht"	X		X	X
Warnungen "Prozesse reagieren nicht" für eine Benutzergruppe	X		X	X
Prozessseiten pro Sekunde	X	X	X	X
Archiv für Prozessleistung	X	X	X	X
Prozessleistungsübersicht nach Prozess	X	X	X	X
Prozessstabilitätsübersicht nach Prozess	X	X	X	X
Prozessübersicht	X	X	X	X
Prozessthreadanzahl	X	X	X	X
Prozessnutzung	X	X	X	X
Archiv für Prozessnutzung	X	X	X	X
Liste mit Echtzeitwarnungen	X	X	X	X
Übersicht über Echtzeitgeräte	X	X	X	X
Echtzeitnetzwerkleistung	X		X	X
Echtzeitsystemvergleich	X	X	X	X
Echtzeitsystemleistung	X	X	X	X
XenApp-Echtzeitübersicht	X	X	X	
Echtzeitübersicht für XenApp-Benutzer	X		X	
Neustarts	X	X	X	
Autom. Sitzungswiederverbindungen			X	X

Berichtsname	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Client- und Serverstartdauer für Sitzung			X	X
Clientstartdauer Sitzung			X	X
Archiv für Clientstartzeit für Sitzung			X	X
Sitzungsclienttyp		X	X	X
Sitzungsanzahlen		X	X	
Sitzungs-CPU			X	X
Sitzungs-CPU für eine Benutzergruppe			X	X
Anmeldezeit bei Sitzung		X	X	
Sitzungsanmeldezeit für eine Benutzergruppe		X	X	
Sitzungsspeichernutzung			X	X
Verwendete Netzwerkbandbreite der Sitzung			X	X
Sitzungsnetzwerkverzögerung			X	X
Sitzungsnetzwerkverzögerung für eine Benutzergruppe			X	X
Netzwerk-Roundtrip-Zeit für Sitzung			X	X
Netzwerk-Roundtrip-Zeit für Sitzung für eine Benutzergruppe			X	X
Sitzungsnetzwerkvolumen			X	X
Sitzungsnetzwerkvolumen für eine Benutzergruppe			X	X
Sitzungsseitenfehler			X	X
Archiv für Sitzungsleistung			X	X
Serverstartdauer Sitzung			X	X
Archiv für Serverstartzeit von Sitzung			X	X
Details für Sitzungsstartdauer			X	X
Standortnetzwerkverzögerung	X		X	X
Standortnetzwerkfehler	X		X	X

Berichtsname	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Sitzungsnetzwerkfehler für eine Benutzergruppe			X	X
Netzwerk-Roundtrip-Zeit für Standort	X		X	X
Standortnetzwerkvolumen	X		X	X
Software-Anlagenänderungen	X	X	X	X
System-CPU	X	X	X	X
System-CPU-Übersicht	X	X	X	X
Systemdatenträgernutzung	X	X	X	X
Archiv für Systemdatenträgernutzung	X	X	X	X
Übersicht über Systemdatenträgernutzung	X	X	X	X
System-Kernel für ein Gerät	X	X	X	X
Systemspeicher für eine Benutzergruppe		X	X	X
Systemspeicherübersicht	X	X	X	X
Systemspeichernutzung	X	X	X	X
Systemseitenfehler	X	X	X	X
Archiv für Systemleistung	X	X	X	X
Archiv für Trace-Ereignis	X	X	X	X
Transaktionsnetzwerk-verzögerung	X		X	X
Netzwerk-Roundtrip-Zeit für Transaktion	X		X	X
Transaktionsnetzwerkvolumen	X		X	X
Transaktionswebfehler	X		X	X
Zähler für Benutzeranmeldungen			X	X
Daten zu Benutzeranmeldungen		X	X	X
Daten zu Benutzeranmeldungen für eine Benutzergruppe		X	X	X
Benutzerübersicht für eine Benutzergruppe			X	X

Berichtsname	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Besuchte Sites	X		X	X
Archiv für XenApp-Umgebungsnutzung		X	X	
Archiv für XenApp-Sitzungsleistung			X	
XenApp-Übersicht		X	X	
Archiv für XenApp-Systemleistung		X	X	
XenApp-Benutzerübersicht			X	
XenDesktop-Übersicht				X
XenDesktop-Benutzerübersicht				X

Warnungen

Warnungsname	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Große Anzahl aktiver Sitzungen		X	X	
Anwendungsfehler	X		X	X
Anwendungsleistung	X	X	X	X
Anwendungsreaktionsfehler			X	
Anwendungsreaktionszeit			X	
Kommunikationsfehler bei Clientaktualisierung		X	X	
Fehler beim Lesen der Datenbankdatei zur Clientaktualisierung		X	X	
Fehler beim Lesen der Clientaktualisierungsdatenbank		X	X	
Fehler beim Lesen des Client-aktualisierungsverzeichnisses		X	X	
Fehler des Dateicache bei der Clientaktualisierung		X	X	
Dateiaufzählungsfehler bei Clientaktualisierung		X	X	

Warnungsname	**Endpunkt**	**XA Standard**	**XA Erweitert**	**Virtuelle Desktops**
Fehler beim Lesen der ICA-Datei bei der Clientaktualisierung		X	X	
Fehler beim Starten der Client-aktualisierungsinstallation		X	X	
Fehler beim Lesen der Installationskonfiguration für Clientaktualisierung		X	X	
Unzureichender Plattenspeicherplatz für Clientaktualisierung		X	X	
Fehler wegen unzureichender Berechtigungen bei Clientaktualisierung		X	X	
Speicherzuordnungsfehler bei Clientaktualisierung		X	X	
Fehler beim Senden der neuen Version bei der Clientaktualisierung		X	X	
Fehler beim Beenden der Clientaktualisierung		X	X	
Upgradefehler bei Clientaktualisierung		X	X	
Konfigurationsprotokollierung sdatenbank nicht verfügbar		X	X	
Desktopregistrierung fehlgeschlagen				X
Geräteneustart	X	X	X	
Dominante Sitzung		X	X	
Zu viele getrennte Sitzungen		X	X	
Fehler bei der Verbindung zum Datenspeicher der Farm		X	X	
Fehler von Systemüberwachung und -wiederherstellung bei der Wiederherstellung		X	X	
Testfehler bei Systemüberwachung- und -wiederherstellung		X	X	
Heartbeat unterbrochen				X

Warnungsname	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Hohe Anwendungsressourcen-nutzung	X	X	X	X
IMA-Dienst reagiert nicht mehr		X	X	
Fehler bei der Verbindung zum Lizenzserver		X	X	
Light-Trace-Ereignis	X		X	X
Max. Anzahl der Farm-verbindungen überschritten		X	X	
Netzwerkverbindungsleistung überstieg SLA	X		X	X
Netzwerk-Socket-Fehler	X		X	X
Netzwerktransaktionsfehler	X		X	X
Netzwerktransaktionsleistung überstieg SLA	X		X	X
Neuer Prozess	X	X	X	X
Anzahl der Server in einer Zone ist zu hoch		X	X	
Ausfall des physikalischen Datenträgers	X		X	
Plug & Play-Hardwareänderung	X		X	X
Fehler der Druckdienste		X	X	X
Prozessausfall	X		X	X
Der Prozess reagiert nicht	X		X	X
Prozess-Snapshot	X		X	X
Beschränkung der gleichzeitigen Nutzung einer veröffentlichten Anwendung		X	X	
Fehler bei der einzelnen Nutzung einer veröffentlichten Anwendung		X	X	
Sitzung getrennt			X	
Sitzung zu lange inaktiv		X	X	
Sitzung deaktiviert		X	X	
Sitzungsleistung (ohne EUEM)			X	

Warnungsname	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Sitzungsleistung		X	X	X
Langsame ICA-Verbindung		X	X	X
Langsame ICA-Verbindung (ohne EUEM)			X	
Engpass bei Systemdatenträger	X	X	X	X
Niedrige Ressourcen	X	X	X	X
Systemleistung:	X	X	X	X
Verlangsamung des Systems	X	X	X	X
Systemüberlastung	X	X	X	X
Fehler bei Clientverbindung zu Terminalserver		X	X	
Fehler bei der Lizenzservererkennung für Terminalserver		X	X	
Überlastete Anwendung	X	X	X	X
Überlastete Sitzung		X	X	
Agent für virtuelle Desktops nicht gestartet				X
Windows-Ereignisprotokoll	X	X	X	X
Windows-Ereignisprotokoll: Anwendungsfehler	X	X	X	X
Windows-Ereignisprotokoll: Fehler bei der Sicherheitsprüfung	X	X	X	X
Windows-Ereignisprotokoll: Systemfehler	X	X	X	X
Wahl des Datenkollektors für eine Zone ausgelöst		X	X	
Wahlen in Zone zu häufig		X	X	

Erfassung von Agentdaten

Datentyp	Endpunkt	XA Standard	XA Erweitert	Virtuelle Desktops
Active Application Monitoring			X	
Anwendungsfehler	X		X	X
Anwendung reagiert nicht	X		X	X
EUEM-/SEMS-Daten			X	X
ICA-Kanal-Leistung			X	X
IMA-Dienststatus		X	X	
Druckdienste			X	X
Sitzungsleistung			X	X
Systemleistung:		X	X	X
Benutzerdefinierte Leistungsüberwachung	X	X	X	X
Geräteanlagenänderungen	X	X	X	X
Datenträgernutzung	X	X	X	X
Light-Trace-Ereignisse	X	X	X	X
Netzwerkleistung:	X		X	X
Netzwerktransaktionen	X		X	X
Prozessabstürze/Snapshots	X		X	X
Prozessleistung	X	X	X	X
Prozessnutzung	X	X	X	X
Remotezugriff für Agent	X	X	X	X
Systemleistung:	X	X	X	X

Registerkarte "Konfigurieren"

Auf der Registerkarte "Konfiguration" werden alle Features für Benutzer mit Administratorprivilegien angezeigt. Es gibt folgende Ausnahmen basierend auf den Agentunterstützungs-Einstellungen:

- Wenn Unterstützung für EdgeSight für XenApp deaktiviert ist, wird die Seite "Farm-Authentifizierung" nicht angezeigt.
- Wenn Unterstützung für EdgeSight für XenApp auf "Standard" gesetzt oder deaktiviert ist, wird die Seite "IP-Bereiche" nicht angezeigt.
- Wenn nur Unterstützung für EdgeSight für virtuelle Desktops aktiviert ist, wird die Seite "Lizenzierung" nicht angezeigt.

Unterstützung für Active Application Monitoring

Um Active Application Monitoring-Skripte aufzuzeichnen, muss der EdgeSight für XenApp Agent 5.0 im erweiterten Modus ausgeführt werden.

Verfügbarkeit von EdgeSight-Features nach Agentversion

Die Art der gesammelten Daten hängt von der Version des EdgeSight-Agents ab, die auf einem Gerät installiert ist. Manche Berichte und SQL-Ansichten geben keine Daten zurück, wenn die Sammlung des Datentyps nicht vom Agent unterstützt wird.

EdgeSight 4.2-Agents

Auf den Geräten muss ein EdgeSight-Agent der Version 4.2 oder höher ausgeführt werden, damit sie im Dashboard angezeigt werden.

EdgeSight 4.5-Agents

EdgeSight für XenApp bietet feinmaschige Endbenutzererlebnis-Überwachungsdaten (EUEM), die durch die XenApp- oder Presentation Server- und ICA-Client-Instrumentation gesammelt werden. Die Daten beinhalten Messwerte zur Netzwerkbandbreite, ICA-Roundtrip-Zeit, Client- und Serverstartzeit und ICA-Kanalbandbreite. Die Sitzungserlebnis-Überwachungsdaten ersetzen die zuvor gesammelten Sitzungslatenzdaten. Die Sammlung dieser Messobjekte hängt von der folgenden Gruppe von Softwarekomponenten ab:

- EdgeSight 4.5 Agent oder höher wird auf dem XenApp- oder Presentation Server-Computer ausgeführt
- Presentation Server 4.5 oder höher Enterprise oder Platinum Edition
- ICA-Client Version 10 oder höher

Wenn diese Softwarekomponenten nicht auf dem überwachten Gerät vorhanden sind, enthalten die folgenden Berichte und SQL-Ansichten **keine** Daten:

- Berichte
    - Archivierte Daten zur Clientstartzeit einer Gruppe
    - ICA-Roundtrip-Zeit
    - Archivierte Daten für ICA-Roundtrip-Zeit
    - ICA-Datenverkehr für eine Benutzergruppe
    - Archivierte Daten zur Serverstartzeit
    - Clientstartdauer Sitzung
    - Serverstartdauer Sitzung
    - Details für Sitzungsstartdauer
- SQL-Ansichten
    - vw_ctrx_client_start_perf: Leistungsdaten zum Clientstart
    - vw_ctrx_archive_client_start_perf: Archivierte Daten zur Clientstartleistung
    - vw_ctrx_ica_rt_perf: Leistungsdaten zum ICA-Roundtrip
    - vw_ctrx_archive_ica_roundtrip_perf: Archivierte Daten zur ICA-Roundtrip-Leistung
    - vw_ctrx_server_start_perf: Leistungsdaten zum Serverstart
    - vw_ctrx_archive_server_start_perf: Archivierte Daten zur Serverstartleistung

EdgeSight 5.0-Agents

Die folgenden Tools, Berichte und SQL-Ansichten geben nur Daten zurück, wenn EdgeSight Agent Version 5.0 oder höher auf dem überwachten Gerät installiert ist:

- Active Application Monitoring (Agent muss im erweiterten Modus ausgeführt werden)
- Farmüberwachung
- Berichte
  - ICA-Audio-E/A
  - ICA-Laufwerks-E/A
  - ICA-Drucker-E/A
  - Komprimierung der ICA-Sitzung
  - ICA-Sitzungs-E/A
  - ICA-Video-E/A
  - Verfügbarkeit des IMA-Dienstes
  - IMA-Dienststatus
  - Autom. Sitzungswiederverbindungen
- SQL-Ansichten
  - vw_ctrx_session_autoreconnect: Daten zu automatischen Verbindungswiederherstellungen für eine Sitzung
  - vw_ctrx_archive_session_autoreconnect: Archivierte Daten zu automatischen Verbindungswiederherstellungen einer Sitzung
  - vw_ctrx_service_state: ICA-Dienststatus
  - vw_ctrx_archive_service_state: Archivierte Daten zum ICA-Dienststatus
  - vw_ctrx_service_availability: ICA-Dienstverfügbarkeit
  - vw_ctrx_archive_service_availability: Archivierte Daten zur ICA-Dienstverfügbarkeit
  - vw_ctrx_channel_perf: Leistungsdaten zum ICA-Kanal
  - vw_ctrx_archive_channel_perf: Archivierte Daten zur ICA-Kanalleistung

EdgeSight 5.2-Agents

Der EdgeSight für virtuelle Desktops Agent wurde in EdgeSight 5.2 hinzugefügt. Dieser Agent ist erforderlich, um Daten für die folgenden Berichte zu sammeln:

- XenDesktop-Übersicht
- XenDesktop-Benutzerübersicht
- HDX MediaStream-E/A
- HDX Plug-n-Play-E/A

Um Daten für die folgenden neuen Berichte zu sammeln, müssen entweder der EdgeSight für XenApp 5.*x* Agent oder der EdgeSight für virtuelle Desktops 5.2 Agent installiert sein:

- ICA-Client-Version
- Zähler für Benutzeranmeldungen

Wenn ein Agent vor Version 5.2 auf einem virtuellen Desktop installiert wird, werden dieselben Berichte und Warnungen mit Leistungsdaten und Warnungsbedingungen für das Gerät angezeigt wie auf Geräten, auf denen ein EdgeSight für Endpunkte Agent installiert ist. Unter "Registerkarte "Durchsuchen"" auf Seite 86 und "Warnungen" auf Seite 91 finden Sie Listen mit Berichten und Warnungen für EdgeSight für Endpunkte Agents.

In EdgeSight 5.2 wurden eine Reihe neuer SQL-Ansichten hinzugefügt. Definitionen dieser Ansichten finden Sie in der Onlinehilfe im Abschnitt "SQL-Ansichten für virtuelle Desktops". Beachten Sie, dass viele Ansichten von den XenApp- und XenDesktop-Überwachungsfunktionen von EdgeSight gemeinsam verwendet werden. Ansichten mit "vw_vda_*" im Namen können nur Daten von virtuellen Desktops abrufen. Mit Ansichten mit "vw_xa_vda_*" im Namen können Sie Daten von einem XenApp-Server oder einem virtuellen Desktop abrufen. Wählen Sie die Ansicht aus, die am besten den in Ihrer Umgebung vorhandenen Geräten entspricht. Beachten Sie, dass mit EdgeSight zurzeit keine Desktop Delivery Controller (DDC)-Systeme überwacht werden können.

Datensammlung von Presentation Server- oder XenApp-Version

Welche Art von Daten gesammelt und angezeigt wird, hängt von der Version von Presentation Server oder XenApp Server, die überwacht wird, sowie von der Version von EdgeSight Agent, die auf dem Gerät installiert ist, ab. Manche Berichte und SQL-Ansichten geben keine Daten zurück, wenn die Sammlung dieses Datentyps nicht von der überwachten Serverversion oder der Agentversion unterstützt wird.

Berichte

In der folgenden Tabelle wird aufgeführt, für welche Versionen von XenApp oder Presentation Server zusammen mit einem EdgeSight 5.x-Agent Berichte Daten enthalten. In manchen Fällen wird die Anzeige von Daten durch die Verwendung älterer Agentversionen eingeschränkt. Weitere Informationen über die Beziehung zwischen Agentversion und Datensammlung finden Sie unter "Verfügbarkeit von EdgeSight-Features nach Agentversion" auf Seite 96.

Berichtsname	**CPS 4.0**	**CPS 4.5**	**XenApp 5.0**
Warnungsarchiv	X	X	X
Warnungen	X	X	X
Anwendungsreaktionsfehler			X EdgeSight Agent 5.0 SP2 erforderlich
Anwendungsreaktionszeit			X EdgeSight Agent 5.0 SP2 erforderlich
Anwendungsreaktionszeit für einen Test			X EdgeSight Agent 5.0 SP2 erforderlich
Anlagenänderungen	X	X	X
Anlagen eines Geräts	X	X	X
CPU-Nutzungsverwaltung		X	X
Gerätearchiv	X	X	X
Geräteübersicht:	X	X	X
Umgebungsnutzung		X	X

Berichtsname	CPS 4.0	CPS 4.5	XenApp 5.0
Ereignisprotokollwarnungen	X	X	X
Ereignisprotokollwarnungen für eine Benutzergruppe	X	X	X
Hardwarewarnungen	X	X	X
Hardware-Anlagenänderungen	X	X	X
HDX MediaStream-E/A			
HDX Plug-n-Play-E/A			
ICA-Audio-E/A		X	X
ICA-Client-Version			
ICA-Laufwerks-E/A		X	X
ICA-Drucker-E/A		X	X
Komprimierung der ICA-Sitzung		X	X
ICA-Sitzungs-E/A		X	X
ICA-Sitzungs-Latenz	X		
ICA-Sitzungs-Latenz für eine Benutzergruppe	X		
Roundtrip-Zeit für ICA-Sitzung		X	X
Archiv für Roundtrip-Zeit für ICA-Sitzung		X	X
Roundtrip-Zeit für ICA-Sitzung für eine Benutzergruppe		X	X
ICA-Sitzungs-Datenverkehr		X	X
ICA-Sitzungs-Datenverkehr für eine Benutzergruppe		X	X
ICA-Video-E/A		X	X
Verfügbarkeit des IMA-Dienstes		X	X
IMA-Dienststatus		X	X
Archiv für Netzwerkverbindung	X	X	X
Netzwerkübersicht	X	X	X
Netzwerkübersicht nach Standort	X	X	X

Berichtsname	CPS 4.0	CPS 4.5	XenApp 5.0
Archiv für Netzwerktransaktion	X	X	X
Netzwerktransaktionsübersicht	X	X	X
Neue Prozesse	X	X	X
Neue Standorte	X	X	X
Portnetzwerkverzögerung	X	X	X
Netzwerk-Roundtrip-Zeit für Port	X	X	X
Portnetzwerkvolumen	X	X	X
Portwebfehler	X	X	X
Prozess-CPU	X	X	X
Kumulative CPU für Prozess	X	X	X
Prozessfehler	X	X	X
Prozessfehler für eine Benutzergruppe	X	X	X
Prozessorinterne Prozessfehler	X	X	X
Prozessausfälle für eine Benutzergruppe	X	X	X
Prozessspeichernutzung	X	X	X
Prozessnetzwerkverzögerung	X	X	X
Prozessnetzwerkvolumen	X	X	X
Warnungen "Prozess reagiert nicht"	X	X	X
Warnungen "Prozesse reagieren nicht" für eine Benutzergruppe	X	X	X
Prozessseiten pro Sekunde	X	X	X
Archiv für Prozessleistung	X	X	X
Prozessleistungsübersicht nach Prozess	X	X	X
Prozessstabilitätsübersicht nach Prozess	X	X	X
Prozessübersicht	X	X	X
Prozessthreadanzahl	X	X	X
Prozessnutzung	X	X	X

Berichtsname	CPS 4.0	CPS 4.5	XenApp 5.0
Archiv für Prozessnutzung	X	X	X
Liste mit Echtzeitwarnungen	X	X	X
Übersicht über Echtzeitgeräte	X	X	X
Echtzeitnetzwerkleistung	X	X	X
Echtzeitsystemvergleich	X	X	X
Echtzeitsystemleistung	X	X	X
XenApp-Echtzeitübersicht	X	X	X
Echtzeitübersicht für XenApp-Benutzer	X	X	X
Neustarts	X	X	X
Autom. Sitzungswieder-verbindungen		X	X
Clientstartdauer Sitzung		X	X
Archiv für Clientstartzeit für Sitzung		X	X
Sitzungsclienttyp		X	X
Sitzungsanzahlen		X	X
Sitzungs-CPU		X	X
Sitzungs-CPU für eine Benutzergruppe		X	X
Anmeldezeit bei Sitzung		X	X
Sitzungsanmeldezeit für eine Benutzergruppe		X	X
Sitzungsspeichernutzung		X	X
Verwendete Netzwerkbandbreite der Sitzung		X	X
Sitzungsnetzwerkverzögerung		X	X
Sitzungsnetzwerkverzögerung für eine Benutzergruppe		X	X
Netzwerk-Roundtrip-Zeit für Sitzung		X	X
Netzwerk-Roundtrip-Zeit für Sitzung für eine Benutzergruppe		X	X
Sitzungsnetzwerkvolumen		X	X

Berichtsname	CPS 4.0	CPS 4.5	XenApp 5.0
Sitzungsnetzwerkvolumen für eine Benutzergruppe		X	X
Sitzungsseitenfehler		X	X
Serverstartdauer Sitzung		X	X
Archiv für Serverstartzeit von Sitzung		X	X
Details für Sitzungsstartdauer		X	X
Standortnetzwerkverzögerung	X	X	X
Standortnetzwerkfehler	X	X	X
Sitzungsnetzwerkfehler für eine Benutzergruppe	X	X	X
Netzwerk-Roundtrip-Zeit für Standort	X	X	X
Standortnetzwerkvolumen	X	X	X
Software-Anlagenänderungen	X	X	X
System-CPU	X	X	X
System-CPU-Übersicht	X	X	X
Systemdatenträgernutzung	X	X	X
Archiv für Systemdatenträgernutzung	X	X	X
Übersicht über Systemdatenträgernutzung	X	X	X
System-Kernel für ein Gerät	X	X	X
Systemspeicher für eine Benutzergruppe	X	X	X
Systemspeicherübersicht	X	X	X
Systemspeichernutzung	X	X	X
Systemseitenfehler	X	X	X
Archiv für Systemleistung	X	X	X
Archiv für Trace-Ereignis	X	X	X
Transaktionsnetzwerk-verzögerung	X	X	X
Netzwerk-Roundtrip-Zeit für Transaktion	X	X	X
Transaktionsnetzwerkvolumen	X	X	X

Berichtsname	CPS 4.0	CPS 4.5	XenApp 5.0
Transaktionswebfehler	X	X	X
Zähler für Benutzeranmeldungen		X	X
Daten zu Benutzeranmeldungen		X	X
Daten zu Benutzeranmeldungen für eine Benutzergruppe		X	X
Benutzerübersicht für eine Benutzergruppe	X	X	X
Besuchte Sites	X	X	X
Archiv für XenApp-Umgebungsnutzung		X	X
Archiv für XenApp-Sitzungsleistung		X	X
XenApp-Übersicht	X	X	X
Archiv für XenApp-Systemleistung	X	X	X
XenApp-Benutzerübersicht	X	X	X

Erfassung von Agentdaten

Datentyp	CPS 4.0	CPS 4.5	XenApp 5.0
Active Application Monitoring			X
Anwendungsfehler	X	X	X
Anwendung reagiert nicht	X	X	X
EUEM-/SEMS-Daten		X	X
ICA-Kanal-Leistung		X	X
IMA-Dienststatus		X	X
Druckdienste		X	X
Sitzungsleistung	X	X	X
Systemleistung:	X	X	X
Benutzerdefinierte Leistungsüberwachung	X	X	X
Geräteanlagenänderungen	X	X	X

Datentyp	CPS 4.0	CPS 4.5	XenApp 5.0
Datenträgernutzung	X	X	X
Light-Trace-Ereignisse	X	X	X
Netzwerkleistung:	X	X	X
Netzwerktransaktionen	X	X	X
Prozessabstürze/Snapshots	X	X	X
Prozessleistung	X	X	X
Prozessnutzung	X	X	X
Remotezugriff für Agent	X	X	X
Systemleistung:	X	X	X

Integration von EdgeSight mit Microsoft System Center Operations Manager

Dieser Abschnitt enthält Informationen über die Bereitstellung und Konfiguration der Software, die zum Weiterleiten von EdgeSight-Warnungen an Microsoftœ System Center Operations Manager 2007 (SCOM) und zur Überwachung des Zustands von EdgeSight-Servern erforderlich ist. Die erforderliche Software umfasst das Citrix EdgeSight Management Pack und EdgeSight Server 5.2. Zurzeit können nur Warnungen von EdgeSight für XenApp-Agents weitergeleitet werden.

Citrix EdgeSight Management Pack

Das Citrix EdgeSight Management Pack ermöglicht, zusammen mit den EdgeSight-Warnungsaktionsfunktionen, das Weiterleiten von Warnungen von einem EdgeSight-Server an SCOM. Das Management Pack enthält außerdem Monitore, Regeln, Ansichten und Aufgaben für die Überwachung des Zustands von Citrix EdgeSight-Servern.

Beim Import ermittelt das EdgeSight Management Pack alle EdgeSight-Server und implementiert Regeln, die Warnungen vom EdgeSight-Server empfangen und anzeigen.

Das EdgeSight Management Pack umfasst folgende Features:

- Sammeln und Anzeigen von Warnungen, die von EdgeSight Server weitergeleitet wurden
- Überwachen des Zustands der Dienste Citrix RSSH Administratordienst und Citrix RSSH-Anwendungsmanagerdienst
- Remote-Neustarts der Dienste Citrix RSSH-Administratordienst und Citrix RSSH-Anwendungsmanagerdienst, wenn diese beendet wurden
- Sammeln von EdgeSight-Fehlern, die in das Anwendungsereignisprotokoll auf dem EdgeSight-Server geschrieben wurden
- Mehrere Methoden zum Starten der EdgeSight Server Console von der Operations Manager-Betriebskonsole

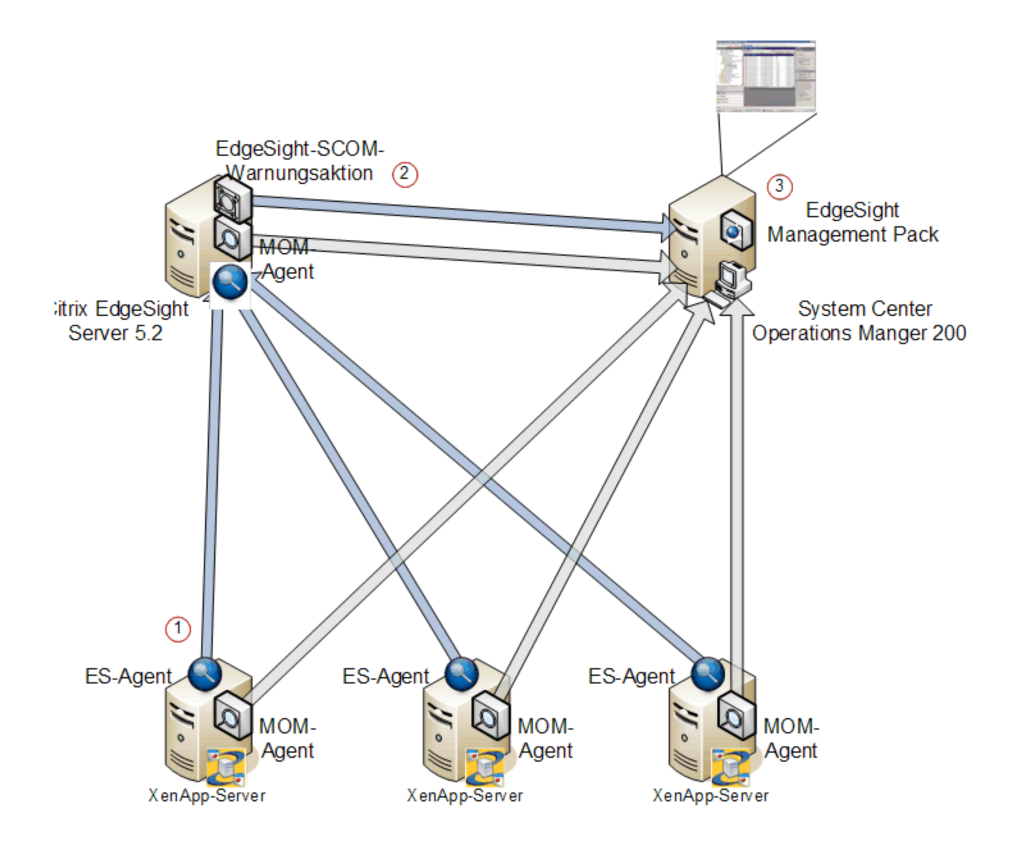
Warnungsaktion "An Microsoft System Center Operations Manager weiterleiten"

Diese EdgeSight-Warnungsaktion dient zum Weiterleiten von EdgeSight-Warnungen an den Operations Manager-Stammverwaltungsserver. Sie können für die Warnungsaktion "An Microsoft System Center Operations Manager weiterleiten" einen Warnungsnamen, einen Stammverwaltungsserver und einen Satz Anmeldeinformationen für die Authentifizierung am Server angeben.

Bereitstellungsdiagramm

Im folgenden Diagramm wird die Kommunikation zwischen Citrix EdgeSight Server und System Center Operations Manager dargestellt. Der EdgeSight Management Pack-Workflow ist folgendermaßen:

1. Der EdgeSight-Agent, der auf einem XenApp-Server ausgeführt wird, erkennt einen Fehlerzustand und gibt eine Warnung an den EdgeSight-Server aus.
2. Eine Warnungsaktion auf dem EdgeSight-Server leitet die Warnung an System Center Operations Manager weiter.
3. Das EdgeSight Management Pack in Systems Center Operations Manager empfängt die EdgeSight-Warnung und zeigt sie in der Operations Manager-Betriebskonsole an; hierbei werden EdgeSight- und SCOM-Warnungen in einer logischen Ansicht zusammengefasst.



Systemanforderungen

Für die Citrix EdgeSight-Warnungsintegration mit System Center Operations Manager ist die Citrix EdgeSight Management Pack-Datei erforderlich, die Sie mit der Betriebskonsole in Operations Manager importieren.

Operations Manager 2007-Server

Um das Management Pack verwenden zu können, müssen Sie Operations Manager 2007 ausführen. Die Mindestanforderungen für Hardware und Software für Operations Manager 2007 finden Sie hier: http://www.microsoft.com/systemcenter/operationsmanager/en/us/system-requirements.aspx.

Sie müssen erst das Citrix XenApp Management Pack v5.0 in Operations Manager importieren, bevor Sie das EdgeSight Management Pack importieren. Das XenApp Management Pack ist auf den XenApp Server Enterprise und Platinum Edition-DVDs verfügbar oder kann von www.citrix.com heruntergeladen werden.

Es ist wichtig, die XenApp Management Pack-Dateien in folgender Reihenfolge in Operations Manager zu importieren:

1. Citrix.Library.mp
2. Citrix.PresentationServer.mp

Citrix.LicenseServer.mp ist ebenfalls Teil des XenApp Management Packs; es wird vom EdgeSight Management Pack aber nicht benötigt.

Hinweis: Sie müssen nach dem Import von Citrix.PresentationServer.mp ein Citrix Administrator-Konto "Ausführung als Profil" mit den Anmelde-informationen des Citrix Administrators konfigurieren. Wird dieser Schritt ausge-lassen, werden Citrix Server u. U. nicht in der Gruppe "Verwaltete Citrix Server" angezeigt. In der Administratordokumentation für das Management Pack für Operations Manager 2007 für XenApp 5.0 für Windows Server 2008 unter # http://support.citrix.com/article/CTX117648 finden Sie detaillierte Anweisungen.

XenApp 5- und Presentation Server 4.x-Server

Sie müssen den Operations Manager-Agent und den Citrix EdgeSight für XenApp Agent auf allen XenApp- und/oder Presentation Server-Computern installieren (siehe *How to Deploy the Operations Manager 2007 Agent Using the Agent Setup Wizard (*http://technet.microsoft.com/en-us/library/bb309515.aspx) beschrieben)).

Stellen Sie sicher, dass die Discovery der Citrix Server korrekt durchgeführt wurde und dass sie von EdgeSight und Operations Manager überwacht werden.

EdgeSight-Server

Sie müssen den Operations Manager-Agent auf dem EdgeSight-Server installieren, damit Operations Manager die Discovery des Servers durchführen, ihn überwachen sowie Warnungen vom EdgeSight-Server empfangen kann. Eine Installationsanleitung finden Sie in *How to Deploy the Operations Manager 2007 Agent Using the Agent Setup Wizard (*http://technet.microsoft.com/en-us/library/bb309515.aspx).

Sie müssen die Operations Manager-Betriebskonsole installieren, die Bibliotheken enthält, die der EdgeSight-Server für die Kommunikation mit dem Operations Manager-Stammverwaltungsserver benötigt (siehe *How to Deploy an Operations Manager 2007 Operations Console Using the Setup Wizard #* (http://technet.microsoft.com/en-us/library/bb381292.aspx)).

Übersicht der Voraussetzungen

Wichtig: Diese Voraussetzungen werden in der Reihenfolge aufgeführt, in der sie importiert oder installiert werden müssen.

Operations Manager 2007-Server

1. Citrix.Library.mp importieren
2. Citrix.PresentationServer.mp importieren

XenApp-Server

1. EdgeSight-Agent installieren
2. Operations Manager-Agent installieren

EdgeSight-Server

1. Operations Manager-Agent installieren
2. Operations Manager-Betriebskonsole oder Operations Manager Authoring Console installieren

Importieren des EdgeSight Management Packs

So importieren Sie das Management Pack

1. Öffnen Sie das EdgeSight-Medium, klicken Sie auf "CD durchsuchen" und gehen Sie zu \installers\Management_Packs.
2. Suchen Sie die Datei Citrix.EdgeSight.mp und kopieren Sie sie auf allen Computern, auf denen die Operations Manager-Betriebskonsole ausgeführt wird, in den Management Pack-Standardordner # (%ProgramFiles%\System Center Management Packs\).
3. Melden Sie sich am Operations Manager-Server an und öffnen Sie die Betriebskonsole.
4. Klicken Sie im Ansichtsbereich auf **Verwaltung**. Klicken Sie in der Verwaltungsansicht auf **Management Packs**.
5. Klicken Sie im Menü **Aktionen** auf **Management Pack(s) importieren**.
6. Gehen Sie zu der Management Pack-Datei **Citrix.EdgeSight.mp** und klicken Sie auf **Öffnen**.
7. Das Dialogfeld **Management Packs importieren** wird angezeigt.
8. Klicken Sie auf **Importieren**.
9. Nachdem das Management Pack erfolgreich installiert wurde, stellt Operations Manager es automatisch auf allen verwalteten Computern in Ihrer Verwaltungsgruppe bereit. Planen Sie ausreichend Zeit ein, um diesen Prozess abzuschließen.

Konfigurieren der Warnungsaktion

So konfigurieren Sie Citrix EdgeSight Server zum Weiterleiten von Warnungen an SCOM

1. Öffnen Sie die EdgeSight Server Console.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter Unternehmenskonfiguration **Warnungen** > **Aktionen**.
4. Klicken Sie dann auf die Schaltfläche **Neue Warnungsaktion erstellen**.
5. Wählen Sie die Option **An Microsoft System Center Operations Manager weiterleiten** und klicken Sie dann auf die Schaltfläche **Weiter**, um den Assistenten zum Erstellen von Warnungsaktionen zu starten.
6. Wenn Sie eine vorhandene Konfiguration (Name und Anmelde-informationen von Stammverwaltungsserver) verwenden möchten, wählen Sie eine aus der Dropdownliste aus. Gehen Sie andernfalls zum nächsten Schritt.
7. Geben Sie den Namen oder die IP-Adresse des Stammverwaltungsservers für System Center Operations Manager ein. Ein vollqualifizierter Domänenname (FQDN) ist nur erforderlich, wenn er zum Herstellen einer Verbindung zwischen dem EdgeSight-Server und dem Stammverwaltungs-server benötigt wird.
8. Geben Sie die Anmeldeinformationen ein, die für die Authentifizierung am Server verwendet werden sollen.
9. Klicken Sie auf die Schaltfläche **Weiter**, wenn Sie die Warnungsaktions-eigenschaften eingerichtet haben.
10. Überprüfen Sie die Warnungsaktion und klicken Sie auf **Fertig stellen**, um zu speichern.

Nach der Erstellung einer Warnungsaktion müssen Sie sie einer Warnungsregel zuweisen.

Zuweisen von Warnungsaktionen zu Warnungsregeln

So weisen Sie die Warnungsaktion einer Warnungsregel zu

1. Klicken Sie auf die Registerkarte **Konfigurieren**.
2. Klicken Sie unter **Warnungen** > **Regeln** auf das Symbol zum Bearbeiten einer vorhandenen Warnungsregel, um den Assistenten für Warnungsregeln zu starten.
3. Wählen Sie **Ändern Sie Zuordnungen von Warnungsregeln zu Warnungsaktionen** und klicken Sie auf die Schaltfläche **Weiter**.
4. Wählen Sie auf der Seite "Warnungsregel einer Abteilung zuweisen" **Alle** oder eine bestimmte Abteilung, der Sie die Regel zuweisen möchten, und klicken Sie dann auf die Schaltfläche **Weiter**.
5. Wählen Sie auf der Seite "Aktionen einer Warnungsregel zuweisen" die Option **Wählen Sie die Warnungsaktionen aus, die dieser Warnungsregel zugeordnet werden sollen**, überprüfen Sie die Warnungsaktion, die Sie im vorherigen Abschnitt erstellt haben und klicken Sie auf die Schaltfläche **Fertig stellen**.

Deinstallieren des EdgeSight Management Packs

Sie können das Management Pack mit der Operations Manager-Betriebskonsole deinstallieren. Durch Deinstallieren des Management Packs werden alle Verweise darauf aus der Operations Manager-Datenbank entfernt, einschließlich der vom Management Pack zur Verfügung gestellten Überwachungsobjekte sowie aller dynamisch ermittelten Ereignis-, Leistungs- und Warnungsdaten. Weitere Informationen über das Deinstallieren von Management Packs finden Sie in der Operations Manager-Dokumentation.

Verwenden des Management Packs

In diesem Kapitel werden die Citrix EdgeSight-Ansichten, -Regeln, -Monitore und -Aufgaben erläutert, die im Management Pack enthalten sind. Außerdem wird beschrieben, wie Sie das Management Pack für Ihre Site konfigurieren können. Folgende Themen werden behandelt:

- Mit Citrix verwaltete Objekte
- Citrix Ansichten
- Starten der Citrix EdgeSight Management Console

Mit Citrix verwaltete Objekte

Die Management Packs von Citrix überwachen eine Reihe Citrix spezifischer Objekte und erstellen Berichte darüber (siehe Tabelle 1).

Objekt	Beschreibung
Citrix Bereitstellung	Stellt eine ermittelte Citrix Bereitstellung dar, die aus mehreren Farmen, Zonen und EdgeSight-Servern bestehen kann.
Verwaltete Citrix Server	Stellt einen von Operations Manager überwachten XenApp- oder Presentation Server-Computer dar. Ein verwalteter Server muss ein Server sein, auf dem eine Version von Presentation Server, die unter "Verwaltete Citrix XenApp-Server" auf Seite 117 aufgeführt wird, mit der entsprechenden Lizenz ausgeführt wird. Auf dem Server muss außerdem der Presentation Server Provider ausgeführt werden.
Nicht unterstützter Citrix Server	Stellt einen nicht von Operations Manager überwachten Server dar. Auf einem nicht unterstützten Server wird keine der unter "Verwaltete Citrix XenApp-Server" auf Seite 117 aufgeführten Versionen von Presentation Server ausgeführt.
Nicht lizenzierte Citrix Server	Stellt einen nicht von Operations Manager überwachten Server dar. Auf dem Server wird der Presentation Server Provider ausgeführt, aber er besitzt keine oder eine ungültige Lizenz. Hinweis: Operations Manager überprüft Lizenzen auf diesen Servern stündlich.
Citrix EdgeSight-Server	Stellt einen von Operations Manager überwachten EdgeSight-Server dar. Auf dem Server muss EdgeSight für XenApp 5.0 oder höher mit einer entsprechenden Lizenz ausgeführt werden.
Citrix Serveranwendung	Eine abstrakte Klasse, die einen Server darstellt, auf dem ein Serverprodukt von Citrix ausgeführt wird. Diese Klasse ist das Ziel für von EdgeSight weitergeleitete Warnungen.

Verwaltete Citrix XenApp-Server

Ein verwalteter Citrix XenApp-Server im Management Pack (angezeigt als Citrix Presentation Server) ist ein Server, auf dem eine der folgenden Versionen von Presentation Server mit einer entsprechenden Lizenz ausgeführt wird:

- Citrix Presentation Server 4.0, Enterprise Edition
- Citrix Presentation Server 4.5, Enterprise oder Platinum Edition
- Citrix XenApp Server 5.0, Enterprise oder Platinum Edition

Server, auf denen frühere Versionen von XenApp/Presentation Server ausgeführt werden, gelten als nicht unterstützte Computer, während Server, die nicht über ausreichende Lizenzen verfügen, als nicht lizenzierte Computer gelten. Diese Computer werden nicht vom Management Pack überwacht und werden nicht im Bereitstellungstopologiediagramm angezeigt.

Hinweis: Nach der Zuweisung von Lizenzen werden Presentation Server-Computer möglicherweise erst nach der nächsten Attribut-Discovery als verwaltete Computer erkannt. Standardmäßig findet dies alle 60 Minuten statt.

Citrix Ansichten

Das EdgeSight Management Pack übernimmt und integriert Citrix Ansichten, die im Citrix XenApp Management Pack zur Verfügung stehen. Mit diesen Ansichten können Sie Ereignisse überwachen, die von Operations Manager und EdgeSight für Server und Serverfarmen ausgegeben werden, auf denen Citrix XenApp und Presentation Server ausgeführt wird.

Das Citrix EdgeSight Management Pack erweitert die Ansichten "Aktive Citrix Warnungen", "Alle Citrix Ereignisse", "Citrix Bereitstellungsstatus" und "Citrix Presentation Server-Topologiediagramm". Außerdem wird hiermit der Citrix EdgeSight-Ordner hinzugefügt, der die Ansichten "Citrix EdgeSight-Warnungen", "Citrix EdgeSight Console" und "Citrix EdgeSight-Status" enthält. Die Ansichten "Citrix Leistung" und "Citrix Lizenzierung" werden vom EdgeSight Management Pack nicht beeinflusst.

Warnungs- und Ereignisansichten

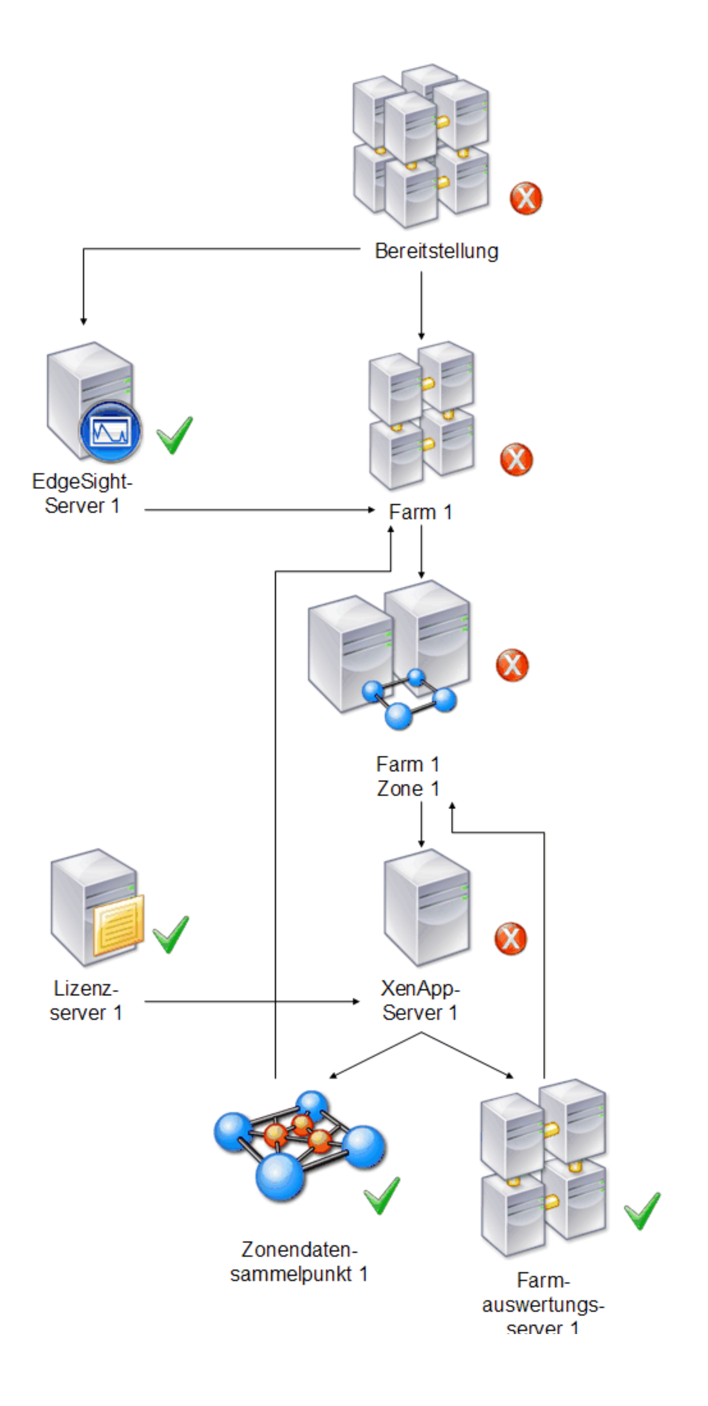
Warnungs- und Ereignisansichten bieten Systemadministratoren Echtzeitdaten über Ereignisse und Warnungen. Warnungen werden in den Ansichten nach Schweregrad und Ereignisse werden chronologisch sortiert, um optimale Übersichtlichkeit zu erreichen.

in diesen Ansichten werden von den XenApp Management Pack-Regeln und -Monitoren generierte Warnungen und Ereignisse und vom EdgeSight-Server weitergeleitete Warnungen gesammelt und angezeigt. Es gibt drei Citrix Warnungs- und Ereignisansichten.

Ansicht	Beschreibung
Alle Citrix Ereignisse	Zeigt alle von Citrix Presentation Server-Komponenten ausgegebenen Ereignisse und alle von den EdgeSight-Warnungsaktionen auf verwalteten Servern eingefügten Ereignisse an.
Aktive Warnungen von Citrix Servern	Zeigt nicht aufgelöste Warnungen an, die auf verwalteten Servern von allen Management Packs (nicht nur dem XenApp Management Pack) ausgegeben werden.
Aktive Citrix Warnungen	Zeigt alle nicht aufgelösten Warnungen an, die vom XenApp Management Pack und dem EdgeSight Management Pack ausgegeben werden.

Ansicht für das Citrix Server-Topologiediagramm

Die Ansicht für das Citrix Server-Topologiediagramm ist eine hierarchische Darstellung der Citrix Bereitstellung, in der Farmen, Zonen, Lizenzserver, XenApp-Server, EdgeSight-Server und die Beziehungen zwischen ihnen angezeigt werden.


Bereitstellung
EdgeSight-
Server 1
Farm 1
Farm 1
Zone 1
Lizenz-
server 1
XenApp-
Server 1
Zonendaten-
sammelpunkt 1
Farm-
auswertungs-
server 1

Die Topologie-Ansicht enthält folgende Informationen:

- Name der Farm, der Zone oder des Servers sowie die ermittelten Eigenschaften für alle Objekte. Folgende Eigenschaften werden bei der Discovery für das EdgeSight Server-Objekt ermittelt:
    - EdgeSight-Versionsnummer
    - SQL Server-Name
    - Datenbankname
    - Datenbankversion
    - IP-Adresse
    - URL der EdgeSight-Administratorkonsole
    - Webport
    - Zuletzt aktualisiert
- Der aktuelle Warnungsstatus, der an höhere Elemente in der Struktur weitergegeben werden kann, sodass Statusänderungen auch sichtbar sind, wenn die Ansicht reduziert ist.

Citrix EdgeSight-Ordner

Das EdgeSight Management Pack erstellt einen neuen Citrix EdgeSight-Ordner unter dem Citrix Presentation Server-Stammordner. Der Citrix EdgeSight-Ordner enthält eine Warnungsansicht, eine Konsolenansicht und eine Statusansicht, die spezifische Informationen für den EdgeSight-Server enthalten.

Ansicht	Beschreibung
Citrix EdgeSight-Warnungen	Zeigt alle Warnungen an, die von der Warnungsaktionsfunktion auf dem EdgeSight-Server ausgegeben werden.
Citrix EdgeSight-Server	Zeigt alle ermittelten Citrix EdgeSight-Server und ihren aktuellen Zustand an.

Citrix EdgeSight-Server-Zustandsrollup

Monitore stellen den Zustand eines verwalteten Computers dar, indem sie Regeln nach vordefinierten Kriterien auswerten. Es gibt drei mögliche Zustände: Erfolg, Warnung und Kritisch.

Das EdgeSight Management Pack enthält zwei Windows-Dienst-Monitore; einen für den Citrix RSSH-Administrationsdienst und einen für den Citrix RSSH-Anwendungsmanagerdienst.

Überwachen	Beschreibung
Citrix RSSH-Aggregat	Zustandsrolluprichtlinie, die den schlechtesten Zustand der beiden RSSH-Dienstmonitore anzeigt.
Citrix RSSH-Administrationsdienst	Überwacht den Status des Citrix RSSH-Administrationsdienstes. Der Zustand wird auf Kritisch gesetzt, wenn der Dienst angehalten wird, und auf Fehlerfrei, wenn der Dienst ausgeführt wird. Der Monitor enthält auch eine Wiederherstellungsfunktion, die den Dienst nach der Wiederherstellung remote neu startet und den Monitorstatus zurücksetzt.
Citrix RSSH-Anwendungsmanagerdienst	Überwacht den Status des Citrix RSSH-Anwendungsmanager-dienstes. Der Zustand wird auf Kritisch gesetzt, wenn der Dienst angehalten wird, und auf Fehlerfrei, wenn der Dienst ausgeführt wird. Der Monitor enthält auch eine Wiederherstellungsfunktion, die den Dienst nach der Wiederherstellung remote neu startet und den Monitorstatus zurücksetzt.

Starten der Citrix EdgeSight Console

Um bei der Fehlerbehebung von Warnungen, die vom EdgeSight-Server an Operations Manager weitergeleitet wurden, zu helfen, enthält das EdgeSight Management Pack eine Reihe von Methoden, die EdgeSight Management Console von der Operations Manager-Betriebskonsole zu starten.

So starten Sie die EdgeSight-Konsole

1. Melden Sie sich an der Operations Manager-Betriebskonsole an.
2. Gehen Sie zur Ansicht **Überwachung**.
3. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie in der Ansicht **Citrix Presentation Server-Topologiediagramm** ein EdgeSight-Server-Symbol aus, klicken Sie in der **Detailansicht** auf den Eigenschaftswert **EdgeSight Console-URL** oder klicken Sie im Bereich **Aktionen** auf **EdgeSight Management Console starten**.

- Wählen Sie in der Ansicht **Citrix EdgeSight-Server** einen EdgeSight-Server aus, klicken Sie in der **Detailansicht** auf den Eigenschaftswert **EdgeSight Console-URL** oder klicken Sie im Bereich **Aktionen** auf **EdgeSight Management Console starten**.

Sicherheitsüberlegungen

Dieser Abschnitt enthält Informationen über Operations Manager-Aktionskonten und die Verwendung von Konten mit geringen Privilegien mit dem Citrix EdgeSight Management Pack und der SCOM-Warnungsaktion.

EdgeSight Management Pack

Das EdgeSight Management Pack verwendet das Standard-Agentaktionskonto, das bei der ersten Installation von Operations Manager erstellt wird, für die Discovery und die Ausführung von Regeln, Aufgaben und Monitoren. Standardmäßig verwendet Operations Manager das lokale Systemkonto als Agentaktionskonto. Wenn das Agentaktionskonto als lokales System ausgeführt wird, verfügt es über alle Privilegien, die für die Discovery und die Ausführung von Regeln, Aufgaben und Monitoren erforderlich sind.

Umgebungen mit niedrigen Privilegien

Sie können ein Konto mit niedrigen Privilegien als Agentaktionskonto verwenden. Für die Wiederherstellungsaufgaben sind jedoch höhere Rechte erforderlich. Konten mit niedrigen Privilegien müssen folgende Anforderungen erfüllen:

- Mitglied in der Gruppe lokaler Benutzer
- Rechte für lokale Anmeldung

Folgende Features werden für Agentaktionskonten mit niedrigen Privilegien unterstützt:

- EdgeSight Server-Discovery
- EdgeSight RSSH-Dienstüberwachung
- Starten der EdgeSight Server Console

Folgende Features werden für Agentaktionskonten mit niedrigen Privilegien **nicht** unterstützt:

- Wiederherstellungsaufgabe zum Neustarten des Citrix RSSH-Administrationsdienstes
- Wiederherstellungsaufgabe zum Neustarten des Citrix RSSH-Anwendungsmanagerdienstes

EdgeSight-Warnungsaktion

Die Warnungsaktion umfasst Anmeldeinformationen für die Authentifizierung. Das Konto muss ein Mitglied der Rolle Operations Manager-Administratoren sein, um auf den SDK-Dienst zugreifen zu können. Dieses Konto muss auch ein Mitglied der lokalen Administratorgruppe auf dem EdgeSight-Server sein, damit die Warnungsaktion einen lokalen Prozess erzeugen kann. Der Abschnitt über niedrige Privilegien enthält Informationen über die mindestens erforderlichen Berechtigungen für dieses Konto.

Umgebungen mit niedrigen Privilegien

Folgende Privilegien sind mindestens erforderlich für SCOM-Administratorkonten:

- Domäne: Mitglied der globalen Gruppe "Domänenbenutzer"
- Operations Manager: Mitglied der Rolle Operations Manager-Administratoren
- EdgeSight für XenApp 5.0: Mitglied der Gruppe lokaler Administratoren auf dem EdgeSight-Server

Index

I

K

L

M

N

P

R

S

T

U

V

W

Z